GFI Product Manual

GFI EndPointSecurity™

Administration and Configuration Manual

http://www.gfi.com

info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.
If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.
All product and company names herein may be trademarks of their respective owners.
GFI EndPointSecurity is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Document Version: ESEC-ACM-EN-02.00.01
Last updated: September 6, 2011

Contents

1 Introduction 1

1.1 About portable media device threats 1
1.2 GFI EndPointSecurity - the solution..... 1
1.3 Using this manual..... 2
1.4 Terms used in this manual 2
1.5 GFI EndPointSecurity licensing 3

2 About GFI EndPointSecurity 5

2.1 Introduction 5
2.2 Key features..... 5
2.3 Components of GFI EndPointSecurity..... 6
2.4 How GFI EndPointSecurity works - Deployment and monitoring..... 7
2.5 How GFI EndPointSecurity works - Device access..... 9
2.6 How GFI EndPointSecurity works - Temporary access..... 9
2.7 Supported device categories..... 10
2.8 Supported connectivity ports 11
2.9 Navigating the GFI EndPointSecurity management console 11

3 Creating new protection policies 13

3.1 Introduction 13
3.2 Using the Create Protection Policy wizard 13

4 Deploying protection policies 29

4.1 Introduction 29
4.2 Adding a target computer in the computers list 29
4.3 Assigning a protection policy 32
4.4 Deploying a protection policy 33
4.5 Verifying the deployment of a protection policy 35

5 Monitoring device usage activity 37

5.1 Introduction 37
5.2 Statistics 37
5.3 Activity..... 38

6 Monitoring statuses 43

6.1 Introduction 43
6.2 General 43
6.3 Agents 47
6.4 Deployment 48
6.5 Statistics 50

7 Reporting 51

8 Discovering devices 53

8.1 Introduction 53
8.2 Device Scan 53

9 Customizing protection policies 59

9.1 Introduction 59

9.2 Configuring controlled device categories 59
9.3 Configuring controlled connectivity ports 60
9.4 Configuring power users 61
9.5 Configuring access permissions for device categories 62
9.6 Configuring access permissions for connectivity ports 65
9.7 Configuring access permissions for specific devices 67
9.8 Viewing access permissions 70
9.9 Configuring priorities for permissions 71
9.10 Configuring device blacklist 72
9.11 Configuring device whitelist 75
9.12 Configuring temporary access privileges 78
9.13 Configuring file-type filters 81
9.14 Configuring security encryption 83
9.15 Configuring event logging 85
9.16 Configuring alerts 87
9.17 Setting a policy as the default policy 90

10 Customizing GFI EndPointSecurity 93

10.1 Introduction 93
10.2 Configuring auto discovery settings 93
10.3 Configuring the alerts administrator account 97
10.4 Configuring alerting options 100
10.5 Configuring alert recipients 102
10.6 Configuring groups of alert recipients 104
10.7 Configuring digest report 105
10.8 Configuring database backend 107
10.9 Configuring user messages 109
10.10 Configuring advanced GFI EndPointSecurity options 110

11 Uninstalling GFI EndPointSecurity 113

11.1 Introduction 113
11.2 Uninstalling GFI EndPointSecurity agents 113
11.3 Uninstalling GFI EndPointSecurity application 115

12 Miscellaneous 117

12.1 Introduction 117
12.2 Entering your license key after installation 117
12.3 Checking for newer GFI EndPointSecurity versions 117

13 Troubleshooting 119

13.1 Introduction 119
13.2 Common Issues 119
13.3 Knowledge Base 119
13.4 Web Forum 119
13.5 Request technical support 119
13.6 Build notifications 119
13.7 Documentation 119

14 Glossary 121

15 Appendix 1 - Deployment error messages 123

15.1 Introduction 123
15.2 Deployment error messages 123

Index 125

List of screenshots

Screenshot 1 - GFI EndPointSecurity: management console 12
Screenshot 2 - GFI EndPointSecurity Create Protection Policy wizard: Name step 14
Screenshot 3 - GFI EndPointSecurity Create Protection Policy wizard: Controlled Categories and Ports step 15
Screenshot 4 - Controlled Device Categories options 15
Screenshot 5 - Controlled connectivity ports options 16
Screenshot 6 - GFI EndPointSecurity Create Protection Policy wizard: Global Permissions step 17
Screenshot 7 - GFI EndPointSecurity Create Protection Policy wizard: Storage Devices step 18
Screenshot 8 - File-type Filter options 18
Screenshot 9 - File-type Filter and user options 19
Screenshot 10 - Encryption options - General tab 20
Screenshot 11 - Encryption options - Permissions tab 20
Screenshot 12 - Encryption options - File-type Filter tab 21
Screenshot 13 - GFI EndPointSecurity Create Protection Policy wizard: Logging and Alerting Options step 22
Screenshot 14 - Logging Options - General tab 23
Screenshot 15 - Logging Options - Filter tab 24
Screenshot 16 - Alerting Options - General tab 25
Screenshot 17 - Alerting Options - Configuring users and groups 26
Screenshot 18 - Alerting Options - Filter tab 27
Screenshot 19 - GFI EndPointSecurity Create Protection Policy wizard: Finish step 28
Screenshot 20 - Add Computer(s) options 30
Screenshot 21 - Select Computers options 30
Screenshot 22 - Import computers options 31
Screenshot 23 - Logon Credentials options 32
Screenshot 24 - Assign Protection Policy options 33
Screenshot 25 - Deployment sub-tab 34
Screenshot 26 - Schedule deployment options 35
Screenshot 27 - Deployment History area 36
Screenshot 28 - Agent's Status area 36
Screenshot 29 - Statistics sub-tab 37
Screenshot 30 - Protection Status area 38
Screenshot 31 - Device Usage by Device Type area 38
Screenshot 32 - Device Usage by Connectivity Port area 38
Screenshot 33 - Activity Log sub-tab 39
Screenshot 34 - Activity Log sub-tab - Advanced filtering 40
Screenshot 35 - Logs Browser sub-tab 41
Screenshot 36 - Query Builder options 42
Screenshot 37 - General sub-tab 43
Screenshot 38 - Service Status area 44
Screenshot 39 - Database Backend Status area 44
Screenshot 40 - Alerting Status area 44
Screenshot 41 - General Status area 45
Screenshot 42 - Protection Status area 45
Screenshot 43 - Online Status area 46
Screenshot 44 - Agents' Status area 46
Screenshot 45 - Device Usage area 47
Screenshot 46 - Agents sub-tab 48
Screenshot 47 - Deployment sub-tab 49
Screenshot 48 - Current Deployments area 49
Screenshot 49 - Queued Deployments area 50
Screenshot 50 - Scheduled Deployments area 50
Screenshot 51 - Deployment History area 50
Screenshot 52 - Device Scan sub-tab 53
Screenshot 53 - Options - Logon Credentials tab 54
Screenshot 54 - Options - Scan Ports tab 55
Screenshot 55 - Options - Scan Device Categories tab 55
Screenshot 56 - Computers area 56
Screenshot 57 - Devices list area 57
Screenshot 58 - Devices list area - Add device to devices database 57
Screenshot 59 - Controlled Device Categories options 60
Screenshot 60 - Controlled connectivity ports options 61

Screenshot 61 - Power users options 62
Screenshot 62 - Add permissions options - Control entities 63
Screenshot 63 - Add permissions options - Device categories 63
Screenshot 64 - Add permissions options - Users 64
Screenshot 65 - Add permissions options - Users 64
Screenshot 66 - Add permissions options - Control entities 65
Screenshot 67 - Add permissions options - Connectivity ports 66
Screenshot 68 - Add permissions options - Users 66
Screenshot 69 - Add permissions options - Users 67
Screenshot 70 - Add permissions options - Control entities 68
Screenshot 71 - Add permissions options - Specific devices 68
Screenshot 72 - Add permissions options - Users 69
Screenshot 73 - Add permissions options - Users 69
Screenshot 74 - Protection Policies sub-tab - devices view 70
Screenshot 75 - Protection Policies sub-tab - users view 71
Screenshot 76 - Protection Policies sub-tab - Security area 71
Screenshot 77 - Black list options 73
Screenshot 78 - Select Devices options 73
Screenshot 79 - Select Devices options - Select device serials 74
Screenshot 80 - Select Devices options - Edit Device serials 75
Screenshot 81 - White list options 76
Screenshot 82 - Select Devices options 76
Screenshot 83 - Select Devices options - Select device serials 77
Screenshot 84 - Select Devices options - Edit Device serials 78
Screenshot 85 - Devices Temporary Access icon 79
Screenshot 86 - GFI EndPointSecurity Temporary Access tool 79
Screenshot 87 - Grant temporary access options - Request code 80
Screenshot 88 - Grant temporary access options - Device categories and connection ports 80
Screenshot 89 - Grant temporary access options - Time restrictions 81
Screenshot 90 - File-type Filter options 82
Screenshot 91 - File-type Filter and user options 82
Screenshot 92 - Encryption options - General tab 83
Screenshot 93 - Encryption options - Permissions tab 84
Screenshot 94 - Encryption options - File-type Filter tab 85
Screenshot 95 - Logging Options - General tab 86
Screenshot 96 - Logging Options - Filter tab 87
Screenshot 97 - Alerting Options - General tab 88
Screenshot 98 - Alerting Options - Configuring users and groups 89
Screenshot 99 - Alerting Options - Filter tab 90
Screenshot 100 - Auto Discovery options - Auto Discovery tab 94
Screenshot 101 - Auto Discovery options - Discovery Area tab 95
Screenshot 102 - Auto Discovery options - Actions tab 96
Screenshot 103 - EndPointSecurityAdministrator Properties options - General tab 97
Screenshot 104 - EndPointSecurityAdministrator Properties options - Working Hours tab 98
Screenshot 105 - EndPointSecurityAdministrator Properties options - Alerts tab 99
Screenshot 106 - EndPointSecurityAdministrator Properties options - Member Of tab 99
Screenshot 107 - Alerting Options - Email tab 100
Screenshot 108 - Alerting Options - Network tab 101
Screenshot 109 - Alerting Options - SMS tab 101
Screenshot 110 – Creating New User options - General tab 103
Screenshot 111 - Creating New Group options 104
Screenshot 112 - Digest Report options - General tab 106
Screenshot 113 - Digest Report options - Details tab 106
Screenshot 114 - Database Backend options 108
Screenshot 115 - Maintenance options 109
Screenshot 116 - Custom Messages options 110
Screenshot 117 - Advanced Options - Communication tab 111
Screenshot 118 - Advanced Options - Deployment tab 111
Screenshot 119 - Advanced Options - Agent Security tab 112
Screenshot 120 - Computers sub-tab - delete computer(s) 113
Screenshot 121 - Computers sub-tab - pending uninstall 114
Screenshot 122 - Deployment sub-tab 115
Screenshot 123 - Un-installation information message 115
Screenshot 124 - License key editing message 117

1 Introduction

1.1 About portable media device threats

The key advantage of removable media devices (or portable devices) is easy access. In theory, this may be of great advantage for organizations, but still, it is a well-reported fact that access and security are at opposite ends of the security continuum.

Developments in removable media technology are escalating. Newer versions of portable devices, such as flash memory, have increased in:

- Better storage capacity
- Improved performance
- Easier and faster to install
- Physically small enough to carry in a pocket.

As a result, internal users may deliberately or accidentally:

- Take away sensitive data
- Expose confidential information
- Introduce malicious code (e.g. viruses, Trojans) that can bring the entire corporate network down
- Transfer inappropriate or offensive material on to corporate hardware
- Make personal copies of company data and intellectual property
- Get distracted during work hours.

In an attempt to control these threats, organizations have started to prohibit the use of (personally-owned) portable devices at work. Best practice dictates that you must never rely on voluntary compliance and the best way to ensure complete control over portable devices is by putting technological barriers.

1.2 GFI EndPointSecurity - the solution

GFI EndPointSecurity is the security solution that helps you maintain data integrity by preventing unauthorized access and transfer of content to and from the following devices or connection ports:

- USB Ports (e.g. Flash and Memory card readers, pen drives)
- Firewire ports (e.g. digital cameras, Firewire card readers)
- Wireless data connections (e.g. Bluetooth and Infrared dongles)
- Floppy disk drives (internal and external)
- Optical drives (e.g. CD, DVD)
- Magneto Optical drives (internal and external)
- Removable USB hard-disk drives
- Other drives such as Zip drives and tape drives (internal and external).

Through its technology, GFI EndPointSecurity enables you to allow or deny access and to assign 'full' or 'read only' privileges to:

- Devices (e.g. CD/DVD drives, PDAs).
- Local or Active Directory users/user groups.

With GFI EndPointSecurity you can also record the activity of all devices or connection ports being used on your target computers (including the date/time of usage and by whom the devices were used).

1.3 Using this manual

This user manual is a comprehensive guide aimed at assisting you in creating and deploying GFI EndPointSecurity protection policies. It describes how to use and configure GFI EndPointSecurity to achieve the best possible corporate security.

This manual contains the following chapters:

Chapter 1	**Introduction** Introduces this manual.
Chapter 2	**About GFI EndPointSecurity** Provides basic information on GFI EndPointSecurity and how it works.
Chapter 3	**Creating new protection policies** Provides information on how to create new protection policies using the Create Protection Policy wizard.
Chapter 4	**Deploying protection policies** Provides information on how to deploy protection policies on to target computers.
Chapter 5	**Monitoring device usage activity** Provides information on how to monitor device and port usage activity on protected target computers.
Chapter 6	**Monitoring statuses** Provides information on how to monitor the status of agents deployed on protected target computers.
Chapter 7	**Reporting** Provides information on how to get further information about the GFI EndPointSecurity ReportPack.
Chapter 8	**Discovering devices** Provides information on how to locate and report all devices that are or have been connected to scanned target computers.
Chapter 9	**Customizing protection policies** Provides information on how to configure protection policy settings.
Chapter 10	**Customizing GFI EndPointSecurity** Provides information on how to customize GFI EndPointSecurity settings.
Chapter 11	**Uninstalling GFI EndPointSecurity** Provides information on how to uninstall GFI EndPointSecurity agents and GFI EndPointSecurity application.
Chapter 12	**Miscellaneous** Provides information on licensing and versioning.
Chapter 13	**Troubleshooting** Provides all the necessary information on how to deal with any problems encountered while using GFI EndPointSecurity. Also provides extensive support information.
Chapter 14	**Glossary** Defines technical terms used within GFI EndPointSecurity.
Chapter 15	**Appendix 1 - Deployment error messages** Provides a list of errors displayed during deployment of agents from the management console.

Getting Started Guide

Detailed installation guidelines are provided in the **GFI EndPointSecurity - Getting Started Guide**, which is downloadable from the GFI website:

http://www.gfi.com/esec/esec4gettingstartedguide.pdf

The Getting Started Guide provides detailed information on how to install, set up and test the installation of GFI EndPointSecurity.

1.4 Terms used in this manual

The following terms are used in this manual:

Provides additional information and references essential for the operation of GFI EndPointSecurity.

Provides important information such as warnings and cautions regarding potential issues commonly encountered.

For any technical terms and their definitions as used in this manual, refer to the **Glossary** chapter in this manual.

1.5 GFI EndPointSecurity licensing

For more information on licensing and evaluation, refer to the GFI website at:

http://www.gfi.com/products/gfi-endpointsecurity/pricing/licensing

2 About GFI EndPointSecurity

2.1 Introduction

This chapter provides you with the following information:

- The key features and components of GFI EndPointSecurity
- How GFI EndPointSecurity works
- The device categories and connectivity ports supported by GFI EndPointSecurity

2.2 Key features

GFI EndPointSecurity offers the following main features:

Group-based protection control

In GFI EndPointSecurity you can configure and place computers into groups that are governed by one protection policy. This allows you to configure a single protection policy and apply it to all the computers that are members of that group.

Granular access control

GFI EndPointSecurity enables you to allow or deny access to a specific device as well as to assign (where applicable) 'full' or 'read only' privileges over every supported device (e.g. CD/DVD drives, PDAs) on a user by user basis.

Scheduled deployment

GFI EndPointSecurity allows you to schedule the deployment of protection policies and any related configuration changes without the need to keep to the GFI EndPointSecurity management console open. The deployment feature also handles failed deployments through automatic rescheduling.

Access control

Apart from blocking a range of device categories, GFI EndPointSecurity also allows blocking:

- By file type - for example, allow the user to read *.doc files but block access to all *.exe files.
- By physical port - all devices connected to particular physical ports, for example, all devices connected to USB ports.
- By device ID - block access to a single device based on the unique Hardware ID of the device.

In Microsoft Windows 7, a feature called **BitLocker To Go** can be used to protect and encrypt data on removable devices. GFI EndPointSecurity performs checks on real file types encrypted with Windows 7 BitLocker To Go.

Device whitelist and blacklist

The administrator can define a list of specific devices that are permanently allowed and others that are permanently banned.

Power users

The administrator can specify users or groups who would always have full access to devices that are otherwise blocked by GFI EndPointSecurity.

Temporary access

The administrator is able to grant temporary access to a device (or group of devices) on a particular computer. This feature allows the administrator to generate an unlock code that the

end-user can use to obtain a time-limited access to a particular device or port, even when the GFI EndPointSecurity agent is not connected to the network.

Status dashboard

The dashboard's user interface shows the statuses of live and deployed agents, database and alerting servers, the GFI EndPointSecurity service as well as statistical data with charts.

The main application keeps track of the live agent status by communicating with its deployed agents. Maintenance tasks are performed automatically once an agent goes online.

Active Directory deployment through MSI

From the GFI EndPointSecurity management console it is possible to generate MSI files that can be later deployed using the Group Policy Object (GPO) feature within the Active Directory or other deployment options. An MSI file will contain all the security settings configured in a particular protection policy.

Agent management password

Agent management functions (such as update and un-install) are protected by a user-configurable password. This means that any other GFI EndPointSecurity instances will not have access to the agent management options.

Device discovery

The GFI EndPointSecurity engine can be used to scan and detect the presence of devices on the network, even on computers that are not assigned any protection policy. The information gathered about detected devices can then be used to build security policies and assign access rights for specific devices.

Logs browser

An in-built tool allows the administrator to browse logs of user activity and device usage that is detected by GFI EndPointSecurity.

Alerting

GFI EndPointSecurity allows you to configure e-mail alerts, network messages and SMS messages that can be sent to specified recipients when devices are connected or disconnected, when device access is allowed or blocked and upon service generated events.

Custom messages

When users are blocked from using devices, they are shown popup messages explaining the reasons why the device was blocked. GFI EndPointSecurity allows the customization of these messages.

Database maintenance

To maintain the size of the database backend, GFI EndPointSecurity can be set to backup or delete events older than a custom number of hours or days.

2.3 Components of GFI EndPointSecurity

When you install GFI EndPointSecurity, the following components are set up:

- GFI EndPointSecurity management console
- GFI EndPointSecurity agent.

GFI EndPointSecurity management console

Through the GFI EndPointSecurity management console you can:

- Create and manage protection policies and specify which device categories and connectivity ports are to be controlled.
- Remotely deploy protection policies and agents on to your target computers Grant temporary access to target computers to use specific devices.

- View the device protection status of every computer that is being monitored.
- Carry out scans on target computers to identify devices currently or previously connected.
- Check logs and analyze what devices have been connected to every network computer.
- Keeps track of which computers have an agent deployed and which agents need to be updated.

GFI EndPointSecurity agent

The GFI EndPointSecurity agent is a client-side service responsible for the implementation of the protection policies on the target computer(s). This service is automatically installed on the remote network target computer after the first deployment of the relevant protection policy through the GFI EndPointSecurity management console. Upon the next deployments of the same protection policy, the agent will be updated and not re-installed.

2.4 How GFI EndPointSecurity works - Deployment and monitoring

GFI EndPointSecurity protection policy deployment and monitoring operations can be divided in four logical stages:

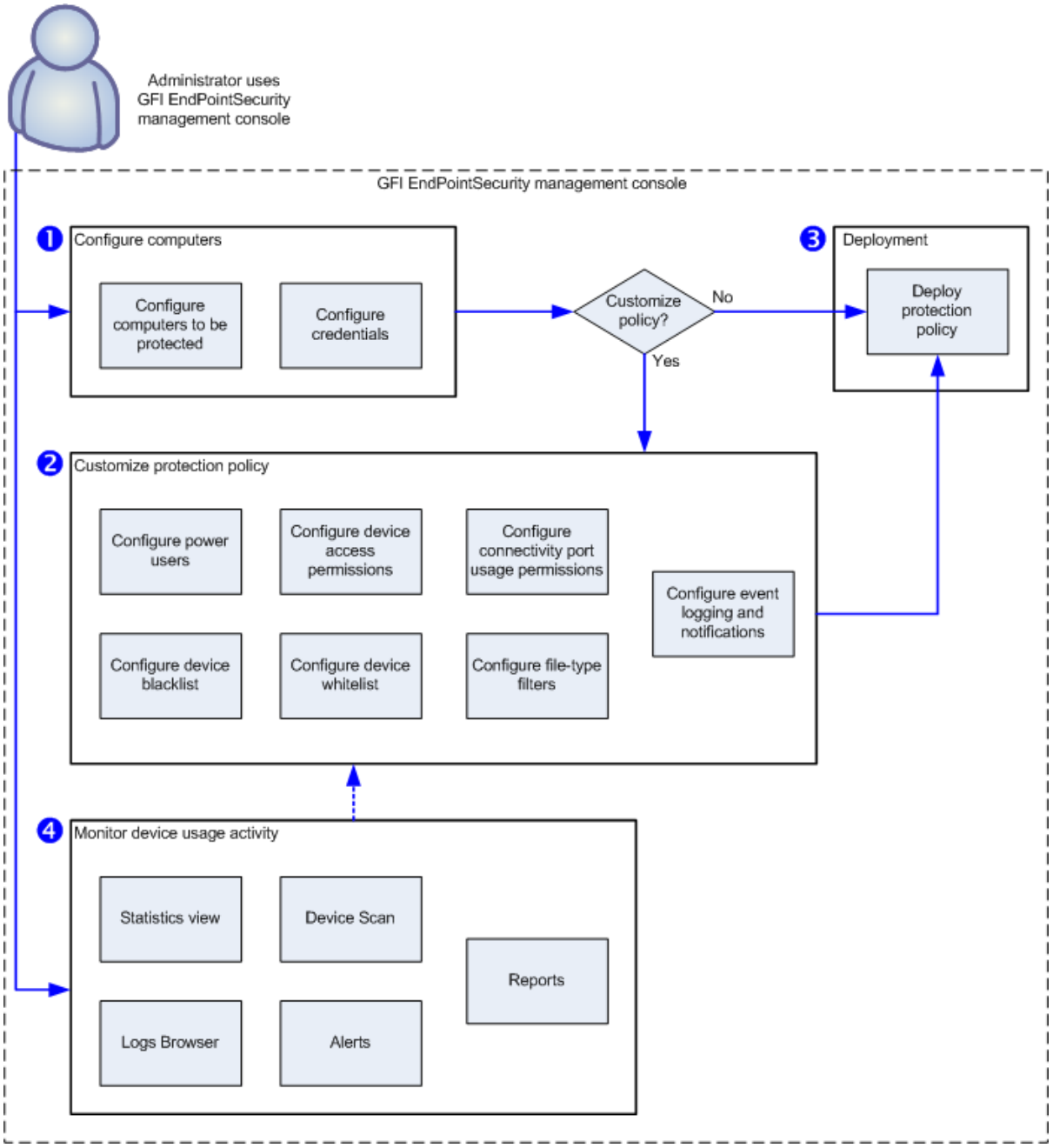


Figure 1 - Protection policy deployment and monitoring

Stage 1 - Configure computers: The administrator specifies which protection policy is assigned to which computers, and the log-on credentials to be used by GFI EndPointSecurity to access the target computers and deploy the agents.

Stage 2 - Customize protection policy: The administrator can customize a protection policy before or after deploying it. Customization options include the creation of power users, addition of blacklisted/whitelisted devices and device access permissions.

Stage 3 - Deploy protection policy: The administrator deploys the protection policy. Upon the first deployment of a protection policy, a GFI EndPointSecurity agent is automatically installed on the remote network target computer. Upon the next deployments of the same protection policy, the agent will be updated and not re-installed.

Stage 4 - Monitor device access: When agents have been deployed, the administrator can monitor all device access attempts via the GFI EndPointSecurity management console, receive alerts and generate reports through the GFI EndPointSecurity ReportPack.

2.5 How GFI EndPointSecurity works - Device access

GFI EndPointSecurity device access operations can be divided in three logical stages:

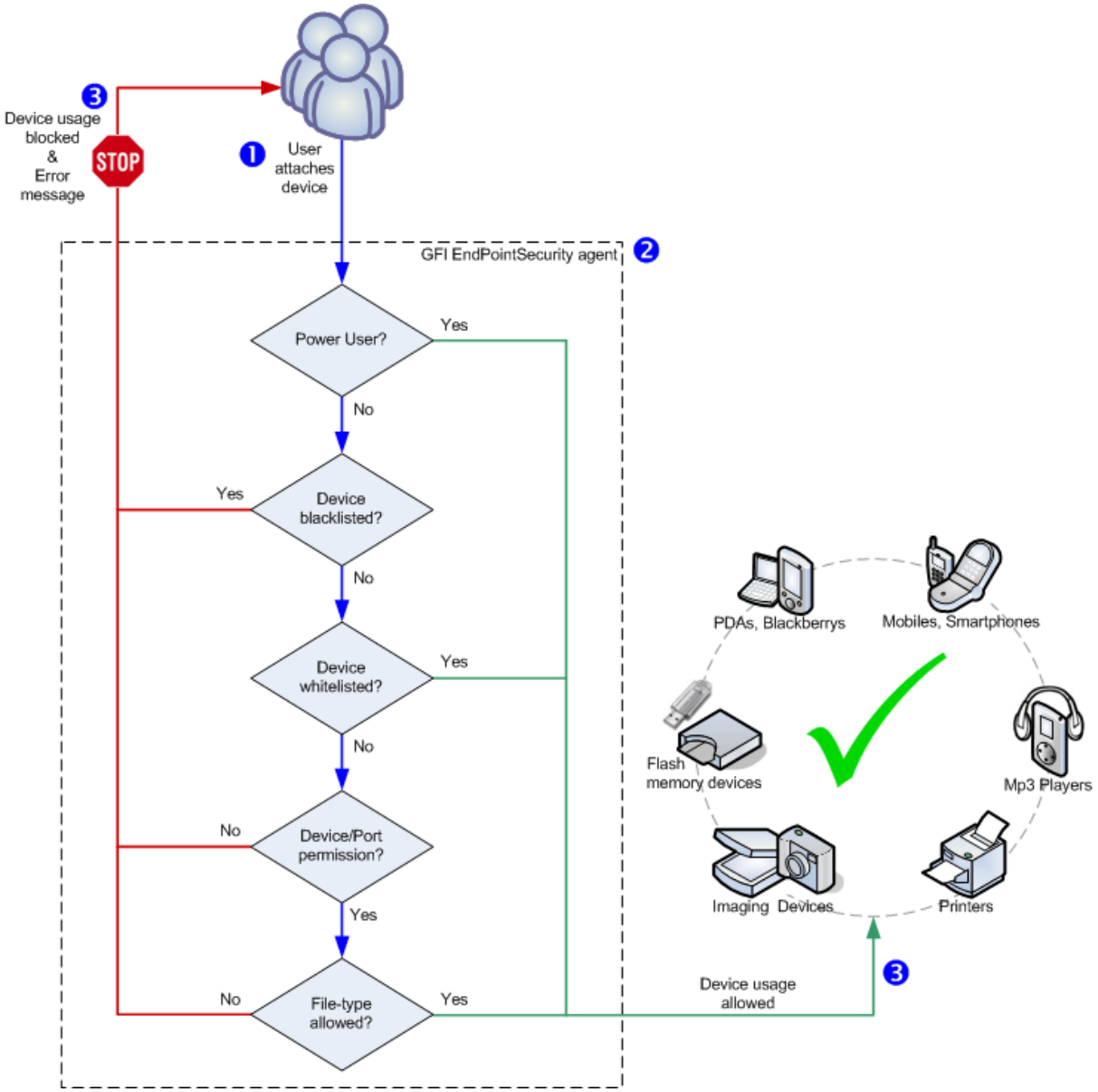


Figure 2 - Device access

Stage 1 - Device attached to computer: The user attaches a device to a target computer protected by GFI EndPointSecurity.

Stage 2 - Protection policy enforcement: The GFI EndPointSecurity agent installed on the target computer detects the attached device and goes through the protection policy rules applicable to the computer/user. This operation determines whether the device is allowed or blocked from being accessed.

Stage 3 - Device usage allowed/blocked: The user either receives an error message indicating that device usage has been blocked, or else is allowed to access the device.

2.6 How GFI EndPointSecurity works - Temporary access

GFI EndPointSecurity temporary access operations can be divided in three logical stages:

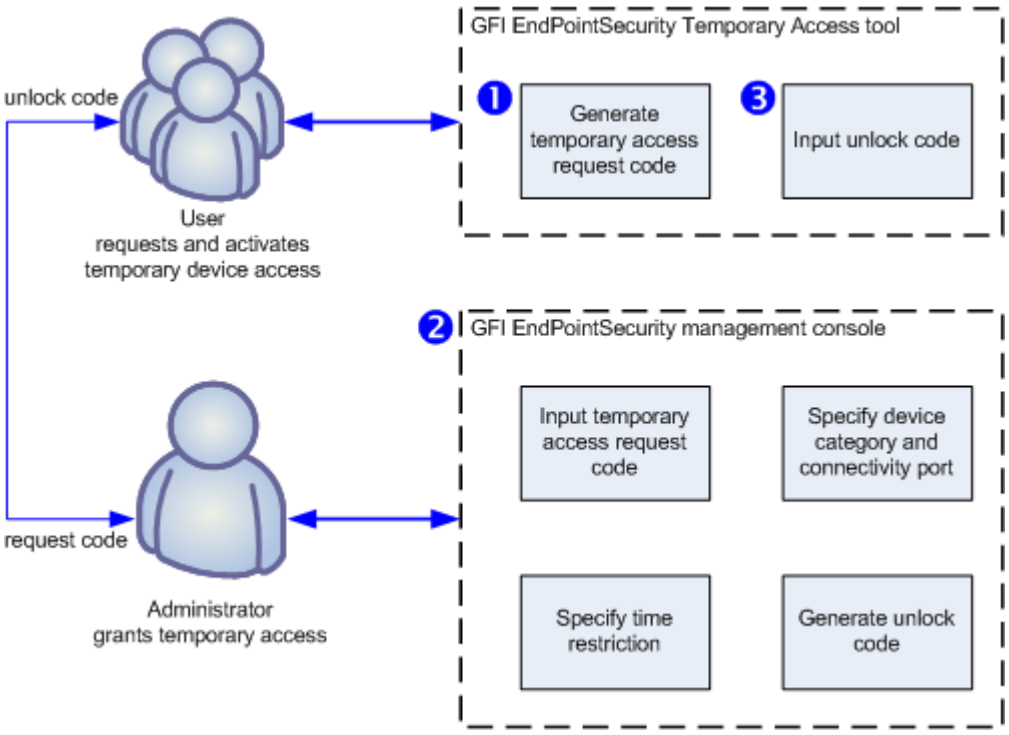


Figure 3 -Requesting/granting temporary access

Stage 1 - User requests temporary device access: The user executes the GFI EndPointSecurity Temporary Access tool from the computer on which the device is to be accessed. The tool is used to generate a request code, which the user communicates with the administrator. The user also needs to inform the administrator on the device types or connection ports that need to be accessed, and for how long will devices/ports access be required.

Stage 2 - Administrator grants temporary access: The administrator uses the Temporary Access feature within the GFI EndPointSecurity management console to enter the request code, specify devices/ports and time restrictions. An unlock code is generated which the administrator then communicates with the user.

Stage 3 - User activates temporary device access: Once the user receives the unlock code sent by the administrator, this code is entered in the GFI EndPointSecurity Temporary Access tool to activate the temporary access and to be able to use the required devices/ports.

2.7 Supported device categories

In GFI EndPointSecurity device categories are organized into the following categories:

- Floppy disks
- CD / DVD
- Storage Devices
  - USB Pen drives
  - Digital Media Players (e.g. MP3/MP4 players)
  - Flash and Memory Card Readers
  - Multi-drive USB devices (i.e. devices that do not mount as a single drive)
  - Other portable storage devices
- Printers
- PDAs
  - Pocket PCs
  - Smart phones
- Network Adapters

- Wi-Fi
- Removable Network Adapters (e.g. USB, Firewire, PCMCIA)

Modems

- Smart phones
- Mobile phones

Imaging Devices

- Digital Cameras
- Webcams
- Scanners

Human Interface Devices

- Keyboards
- Mice
- Game controllers

Other Devices

- Bluetooth dongles/ports
- Infrared dongles/ports
- MO (magneto optical) drives (internal and external)
- Zip drives
- Tape drives.

2.8 Supported connectivity ports

GFI EndPointSecurity scans for devices that are or have been connected on the following ports:

USB

Firewire

PCMCIA

Bluetooth

Serial & Parallel

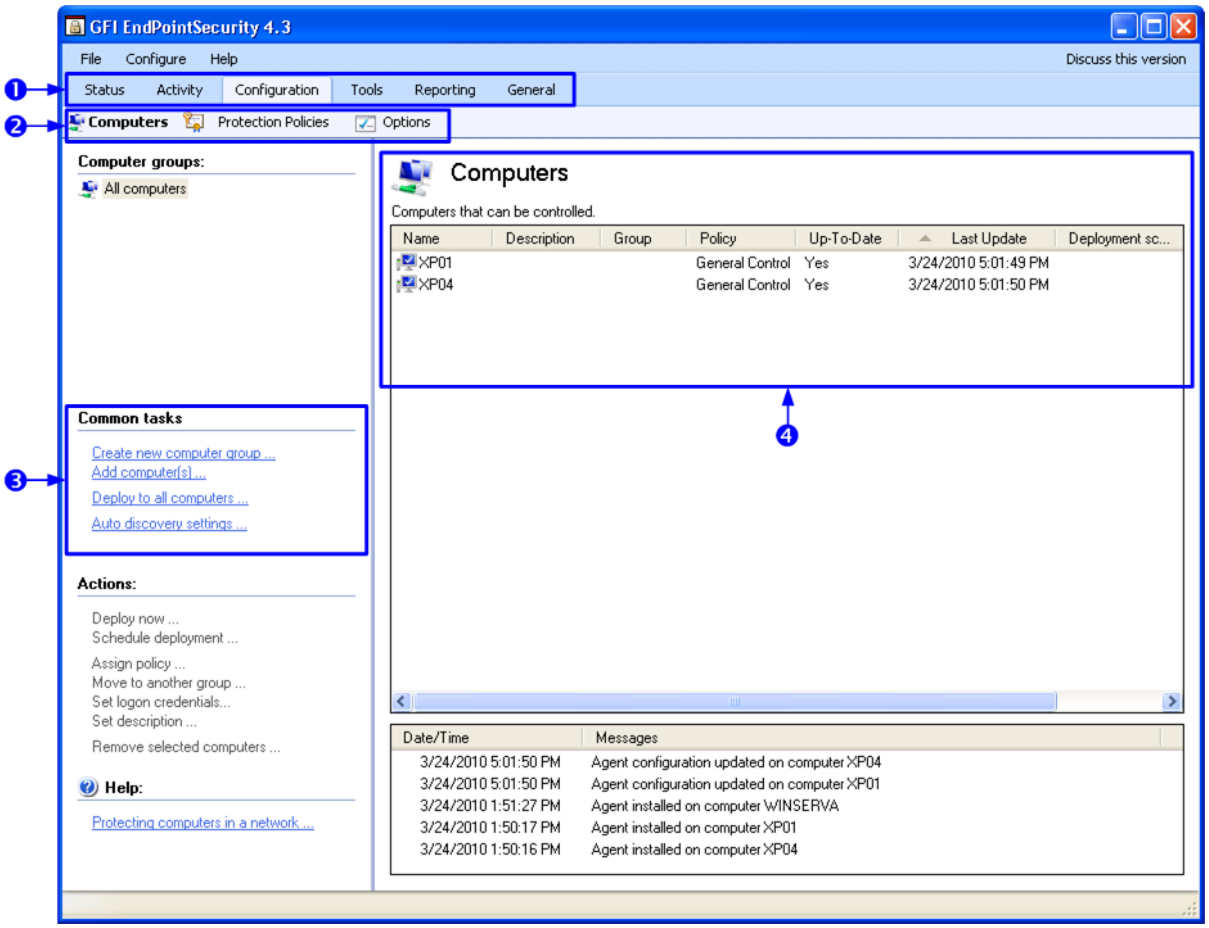
Infrared

Secure Digital (SD)

Internal (e.g. optical drives connected internally on PCI).

2.9 Navigating the GFI EndPointSecurity management console

GFI EndPointSecurity management console provides you with all the administrative functionality to monitor and manage device access usage.



Screenshot 1 - GFI EndPointSecurity: management console

Tabs - Use this feature to navigate between the different tabs within GFI EndPointSecurity management console. The available tabs are:

- **Status** - To monitor the status of GFI EndPointSecurity and statistical information on device access.
- **Activity** - To monitor devices used on the network.
- **Configuration** To access and configure the default protection policies.
- **Tools** - To scan target computers and discover connected devices
- **Reporting** - To see information regarding the GFI EndPointSecurity ReportPack.
- **General** - To check for GFI EndPointSecurity updates, as well as version and licensing details.

Sub-tabs - Use this feature to access more information and settings within GFI EndPointSecurity management console.

Left pane - Use this pane to access the configuration options provided in GFI EndPointSecurity. The configuration options are grouped into several sections, including **Common Tasks**, **Actions** and **Help** sections. Available only for some tabs.

Right pane - Use this pane to configure the configuration options selected from the left pane. Available only for some tabs.

3 Creating new protection policies

3.1 Introduction

GFI EndPointSecurity ships with a default protection policy (shipping default protection policy) so that the software is operational upon installation. You can then create further protection policies to suit your company's device access security policies. In this chapter you will learn how to create protection policies using the Create Protection Policy wizard.

The Create Protection Policy wizard will guide you in configuring the following settings for each protection policy:

- policy name
- establish settings inheritance
- controlled device categories
- controlled ports
- global permissions
- file-type filters
- encryption permissions
- logging options
- alerting options

3.2 Using the Create Protection Policy wizard

Use the Create Protection Policy wizard to create a new protection policy:

Step 1: Launching the Create Protection Policy wizard

To launch the Create Protection Policy wizard:

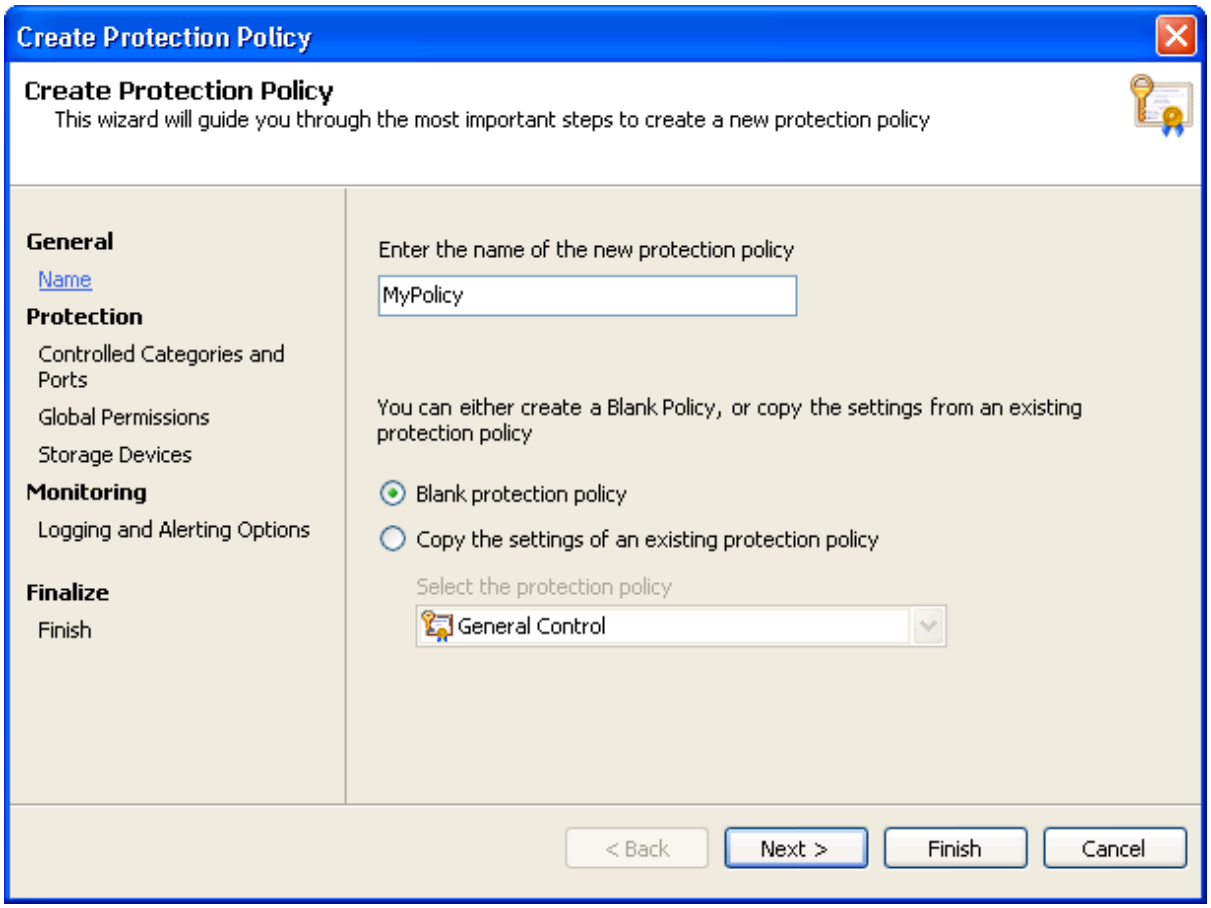
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, click the **Create new protection policy…** hyperlink in the **Common tasks** section.

Step 2: Configuring policy name and establish settings inheritance

GFI EndPointSecurity provides you with the facility to create new protection policies and configure each policy with new settings or else inherit all the settings from an existing protection policy.



Screenshot 2 - GFI EndPointSecurity Create Protection Policy wizard: Name step

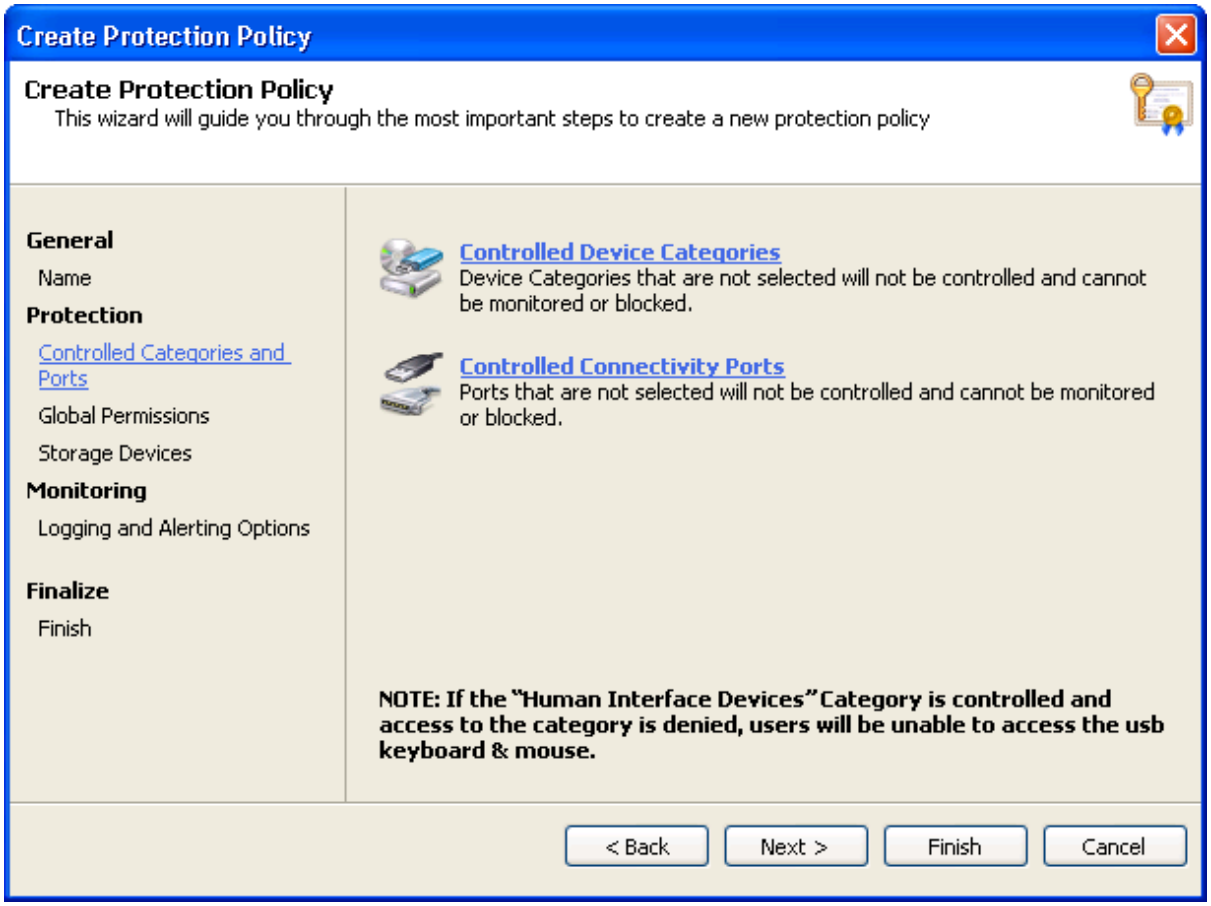
To configure the policy name and establish settings inheritance for this protection policy:

1. Key in a name for the new protection policy.
2. In the settings area select the required settings inheritance option from:
   - » **Blank protection policy** - to create a new protection policy with custom settings.
   - » **Copy the settings of an existing protection policy** - to inherit the settings of an existing protection policy. From the drop-down list select the protection policy from which to inherit the settings. The wizard will go directly to the guidelines page. Review the guidelines page and click **Finish** to complete the wizard.
3. Click **Next**.

Step 3: Configuring controlled categories and ports

GFI EndPointSecurity provides you with the facility to specify which device categories and connectivity ports are to be controlled, monitored and blocked by the protection policy.

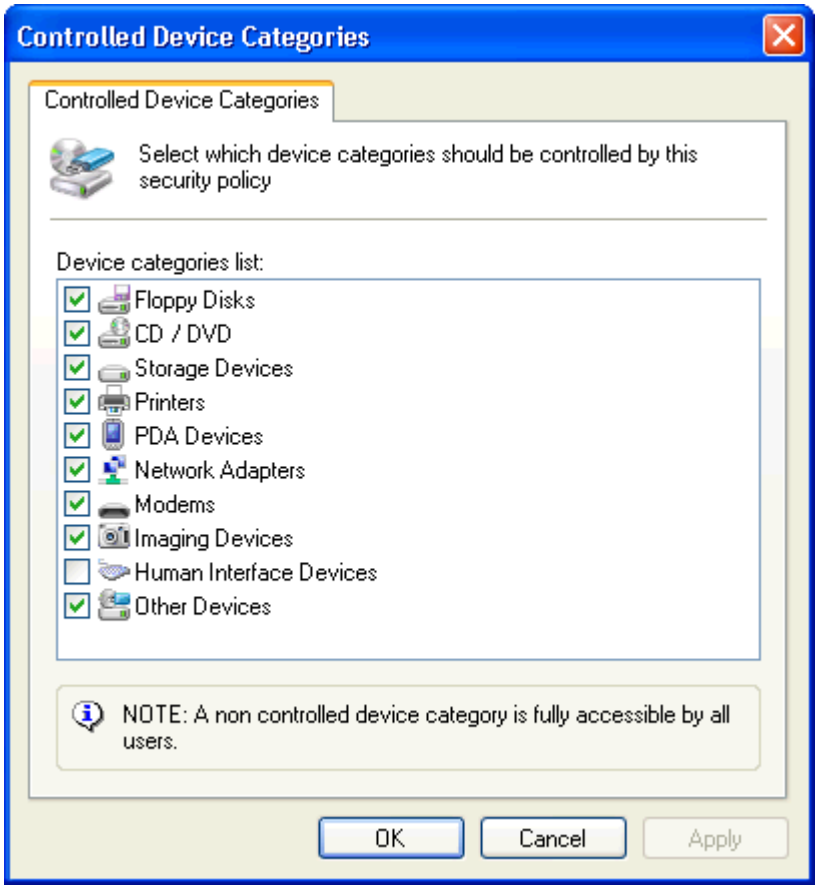
Unspecified devices and ports will be fully accessible from the target computers covered by the protection policy.


Create Protection Policy
Create Protection Policy
This wizard will guide you through the most important steps to create a new protection policy
General
Name
Protection
Controlled Categories and Ports
Global Permissions
Storage Devices
Monitoring
Logging and Alerting Options
Finalize
Finish
Controlled Device Categories
Device Categories that are not selected will not be controlled and cannot be monitored or blocked.
Controlled Connectivity Ports
Ports that are not selected will not be controlled and cannot be monitored or blocked.
NOTE: If the "Human Interface Devices" Category is controlled and access to the category is denied, users will be unable to access the usb keyboard & mouse.
< Back
Next >
Finish
Cancel

Screenshot 3 - GFI EndPointSecurity Create Protection Policy wizard: Controlled Categories and Ports step

To configure which devices and ports will be controlled by this protection policy:

1. Click the **Controlled Device Categories** hyperlink.

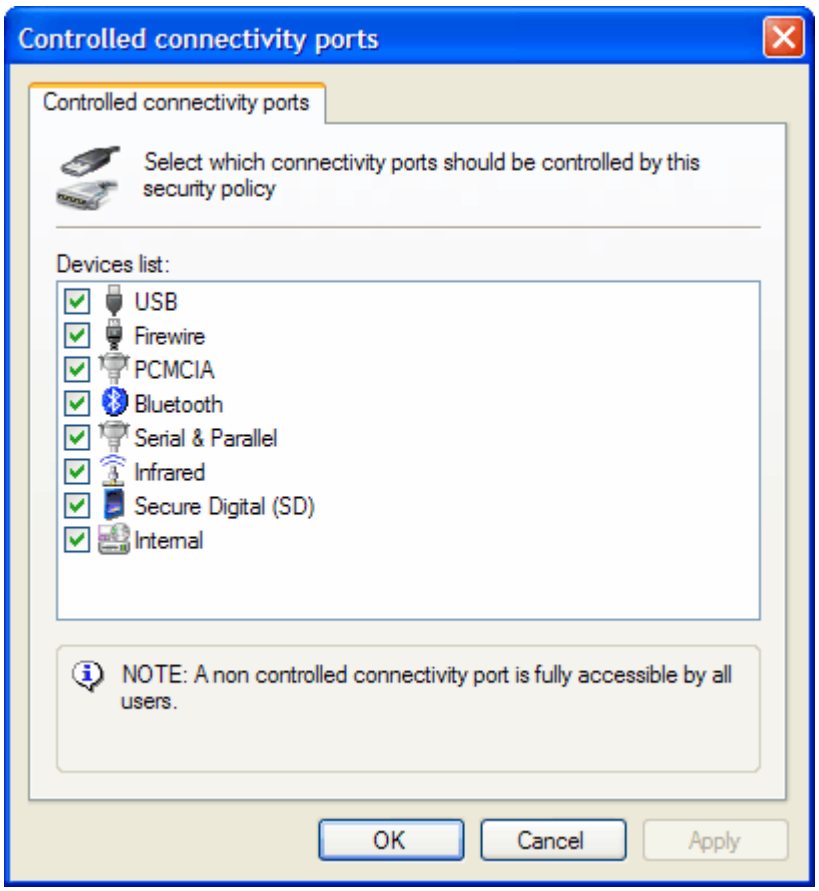


Screenshot 4 - Controlled Device Categories options

2. In the **Controlled Device Categories** dialog, enable or disable the required device categories that will be controlled by the protection policy, and click **OK**.

If **Human Interface Devices** is enabled and access is denied, users will not be able to use USB keyboards and mice connected to target computers protected by this policy.

3. Click the **Controlled Connectivity Ports** hyperlink.



Screenshot 5 - Controlled connectivity ports options

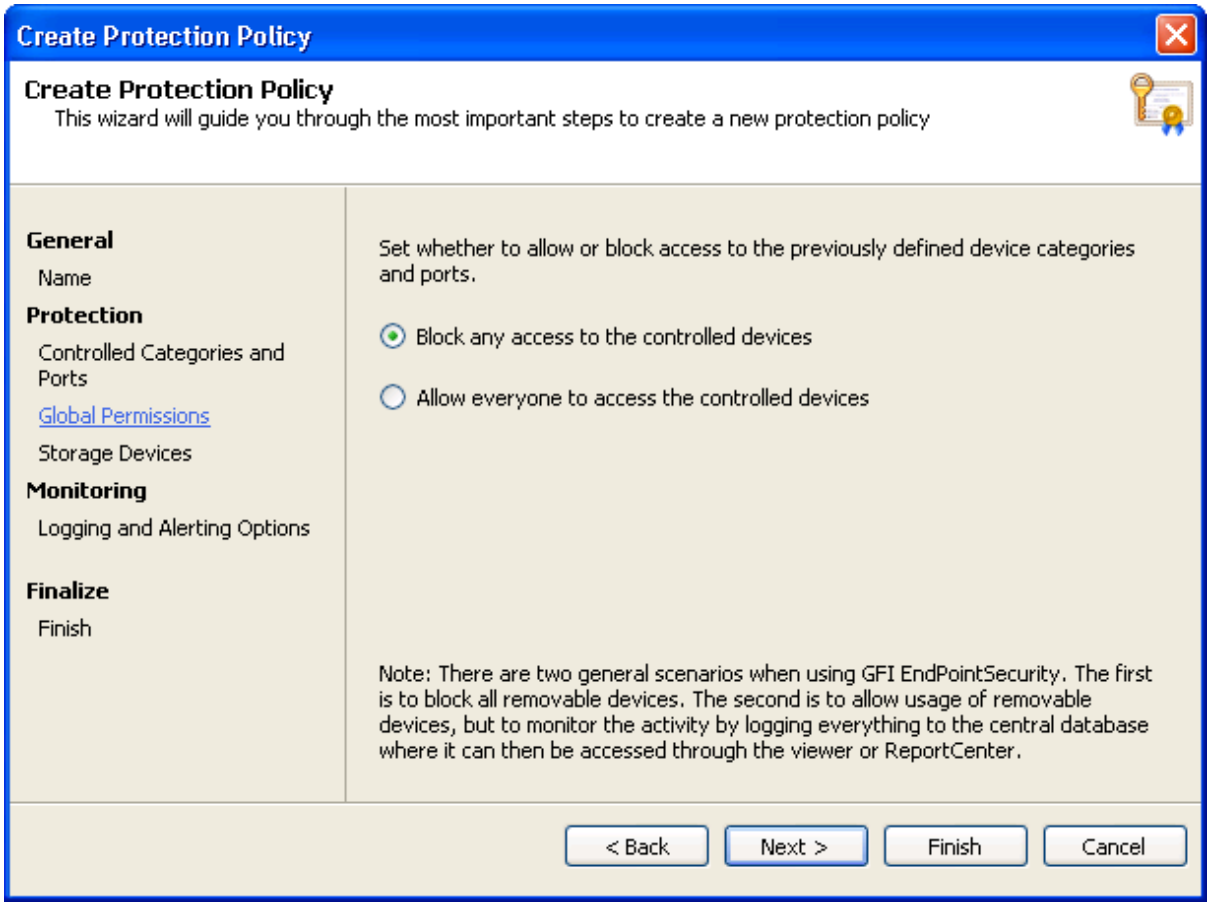
4. In the **Controlled connectivity ports** dialog, enable or disable the required connectivity ports that will be controlled by the protection policy, and click **OK**.

5. Click **Next**.

Step 4: Configuring global permissions

GFI EndPointSecurity provides you with the facility to either block or allow access to all devices falling in a category or which are connected to ports, that were selected in the previous step.

Access can be later blocked/allowed to specific devices, users or target computers. For more information, refer to the **Customizing protection policies** chapter in this manual.


Create Protection Policy
Create Protection Policy
This wizard will guide you through the most important steps to create a new protection policy
General
Name
Protection
Controlled Categories and Ports
Global Permissions
Storage Devices
Monitoring
Logging and Alerting Options
Finalize
Finish
Set whether to allow or block access to the previously defined device categories and ports.
Block any access to the controlled devices
Allow everyone to access the controlled devices
Note: There are two general scenarios when using GFI EndPointSecurity. The first is to block all removable devices. The second is to allow usage of removable devices, but to monitor the activity by logging everything to the central database where it can then be accessed through the viewer or ReportCenter.
< Back
Next >
Finish
Cancel

Screenshot 6 - GFI EndPointSecurity Create Protection Policy wizard: Global Permissions step

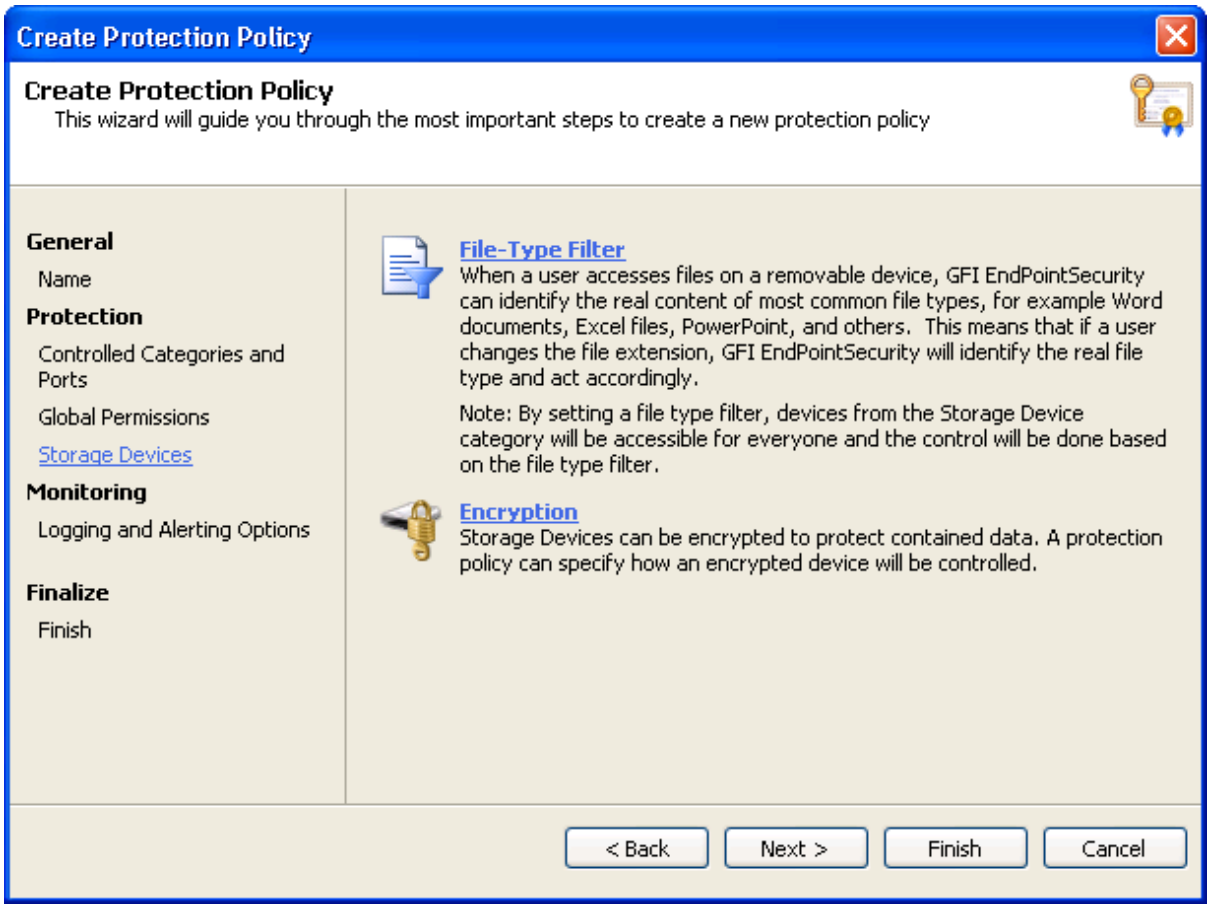
To configure global access permissions for this protection policy:

1. In the permissions area select the required global access permissions option from:
   - » **Block any access to the controlled devices** - to block access to all selected devices/ports.
   - » **Allow everyone to access the controlled devices** - to allow access to all selected devices/ports. If this option is selected, activity monitoring will still be carried out on the target computers covered by the protection policy.
2. Click **Next**.

Step 5: Configuring storage devices

GFI EndPointSecurity provides you with the facility to restrict access based on file-types. GFI EndPointSecurity is also able to identify the real content of most common file-types, (e.g. .DOC or .XLS files), and take the necessary actions applicable for the true file-type. This is most useful when file extensions are maliciously manipulated.

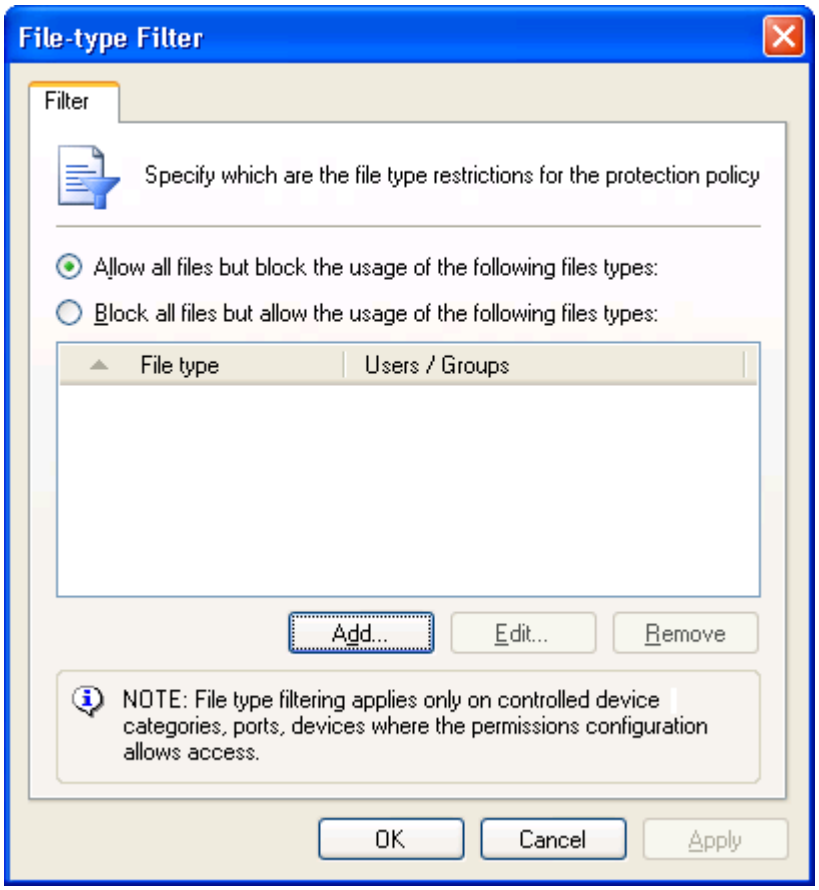
In addition, you can also allow or block Active Directory (AD) users and/or user groups, or local users and/or groups schema from accessing specific file-types stored on devices that are encrypted with BitLocker To Go, a Microsoft Windows 7 feature. These restrictions are applied when the encrypted devices are connected to the target computers covered by the protection policy.


Create Protection Policy
Create Protection Policy
This wizard will guide you through the most important steps to create a new protection policy
General
Name
Protection
Controlled Categories and Ports
Global Permissions
Storage Devices
Monitoring
Logging and Alerting Options
Finalize
Finish
File-Type Filter
When a user accesses files on a removable device, GFI EndPointSecurity can identify the real content of most common file types, for example Word documents, Excel files, PowerPoint, and others. This means that if a user changes the file extension, GFI EndPointSecurity will identify the real file type and act accordingly.
Note: By setting a file type filter, devices from the Storage Device category will be accessible for everyone and the control will be done based on the file type filter.
Encryption
Storage Devices can be encrypted to protect contained data. A protection policy can specify how an encrypted device will be controlled.
< Back
Next >
Finish
Cancel

Screenshot 7 - GFI EndPointSecurity Create Protection Policy wizard: Storage Devices step

To configure restrictions based on file-types and restrictions for devices that are encrypted with BitLocker To Go for this protection policy:

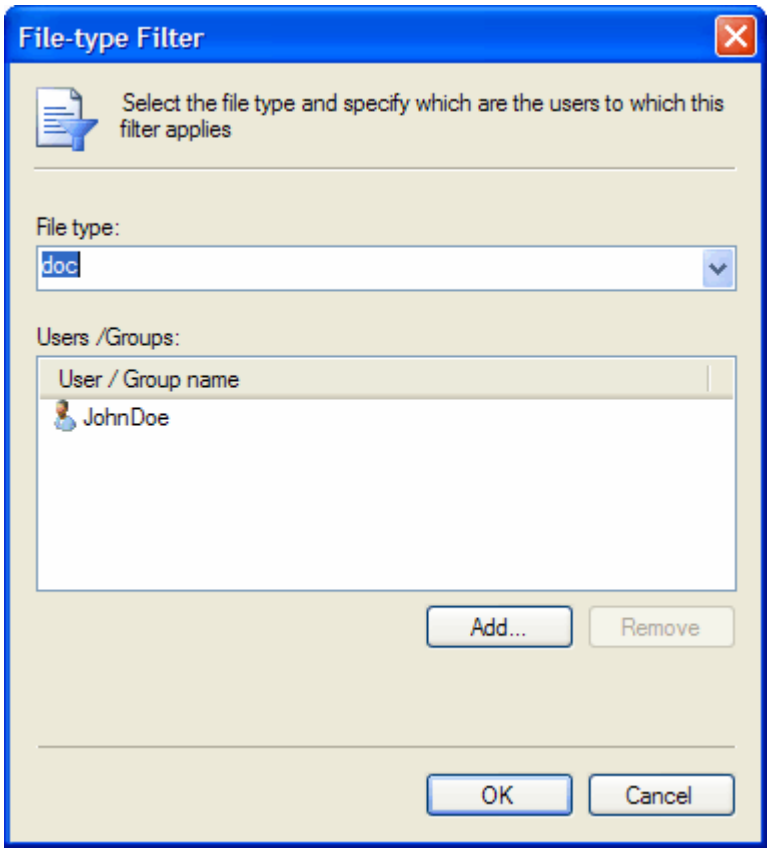
1. Click the **File-Type Filter** hyperlink.


File-type Filter
Filter
Specify which are the file type restrictions for the protection policy
Allow all files but block the usage of the following files types:
Block all files but allow the usage of the following files types:
File type
Users / Groups
Add...
Edit...
Remove
NOTE: File type filtering applies only on controlled device categories, ports, devices where the permissions configuration allows access.
OK
Cancel
Apply

Screenshot 8 - File-type Filter options

2. In the **File-type Filter** dialog, select the restriction to apply to this policy:

- » Allow all files but block the usage of the following file types
- » Block all files but allow the usage of the following file types



Screenshot 9 - File-type Filter and user options

3. Click **Add…** and select or key in the file-type from the **File type** dropdown list.

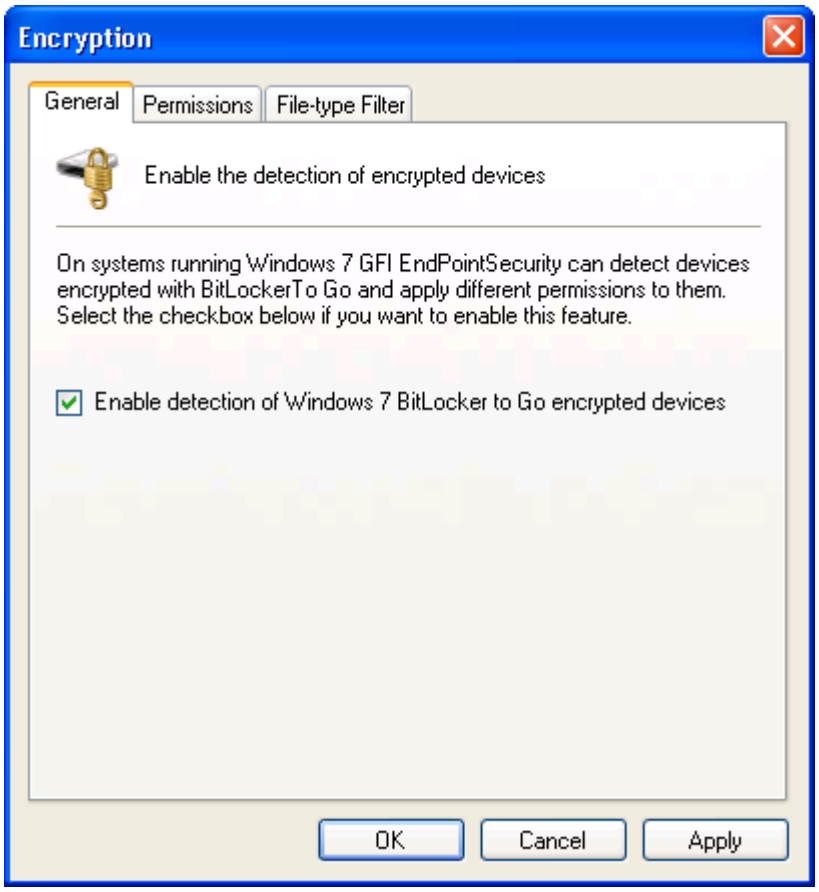
4. Click **Add…** to specify the user(s)/group(s) who are allowed/blocked from accessing the specified file-type, and click **OK**.

Repeat the preceding 2 sub-steps for each file type to restrict.

5. Click **OK** twice.

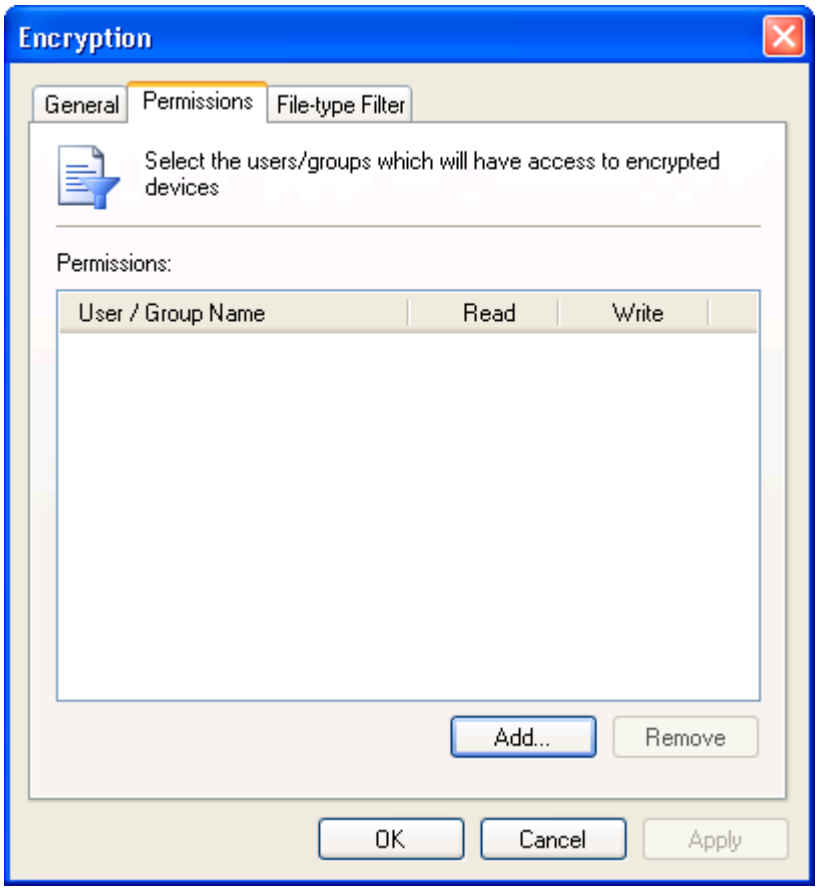
For more information about file extension checks, refer to the **Configuring file-type filters** section in the **Customizing protection policies** chapter.

6. Click the **Encryption** hyperlink.


Encryption
General
Permissions
File-type Filter
Enable the detection of encrypted devices
On systems running Windows 7 GFI EndPointSecurity can detect devices encrypted with BitLockerTo Go and apply different permissions to them. Select the checkbox below if you want to enable this feature.
Enable detection of Windows 7 BitLocker to Go encrypted devices
OK
Cancel
Apply

Screenshot 10 - Encryption options - General tab

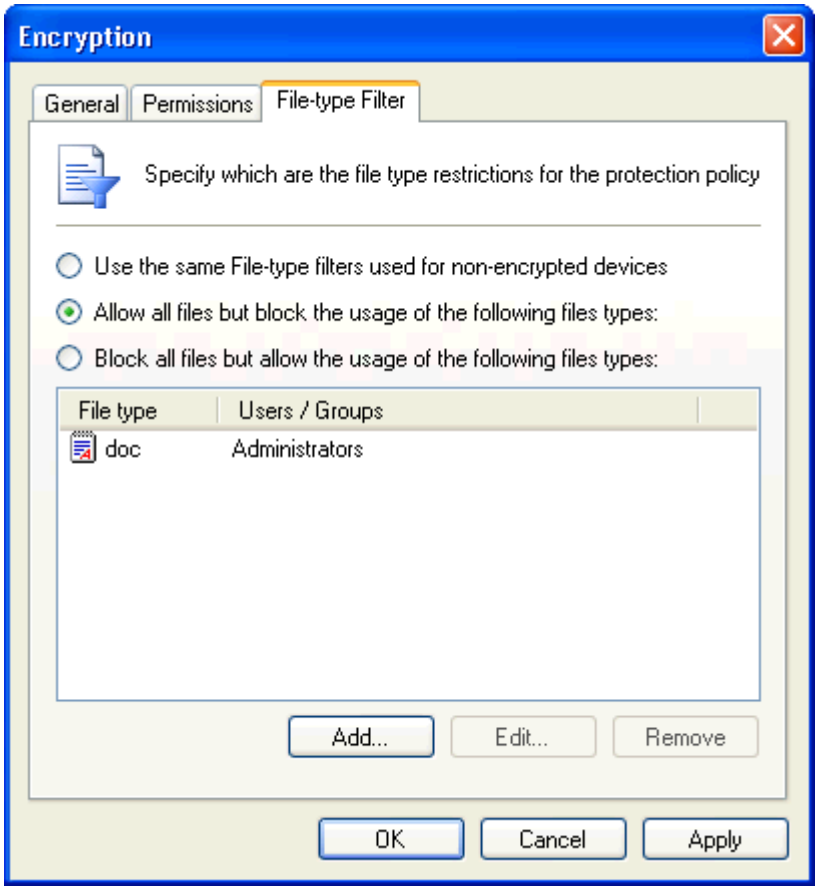
7. In the **Encryption** dialog select the **General** tab and enable or disable **Enable detection of Windows 7 BitLocker To Go encrypted devices** to allow or block the usage of devices that are encrypted with BitLocker To Go.



Screenshot 11 - Encryption options - Permissions tab

8. If the BitLocker To Go option is enabled, select the **Permissions** tab.

9. Click **Add…** to specify the user(s)/group(s) that will have access to the encrypted devices detected by this protection policy, and click **OK**.



Screenshot 12 - Encryption options - File-type Filter tab

10. If the BitLocker To Go option is enabled, select the **File-type Filter** tab to configure the file-types that are to be restricted access.

11. Select the restriction to apply to this policy:

- Use the same File-type filters used for non-encrypted devices
- Allow all files but block the usage of the following file types
- Block all files but allow the usage of the following file types

12. For the last 2 options, click **Add…** and select or key in the file-type from the **File type** dropdown list.

13. Click **Add…** to specify the user(s)/group(s) who are allowed/blocked from accessing the specified file-type, and click **OK**.

Repeat the preceding 2 sub-steps for each file type to restrict.

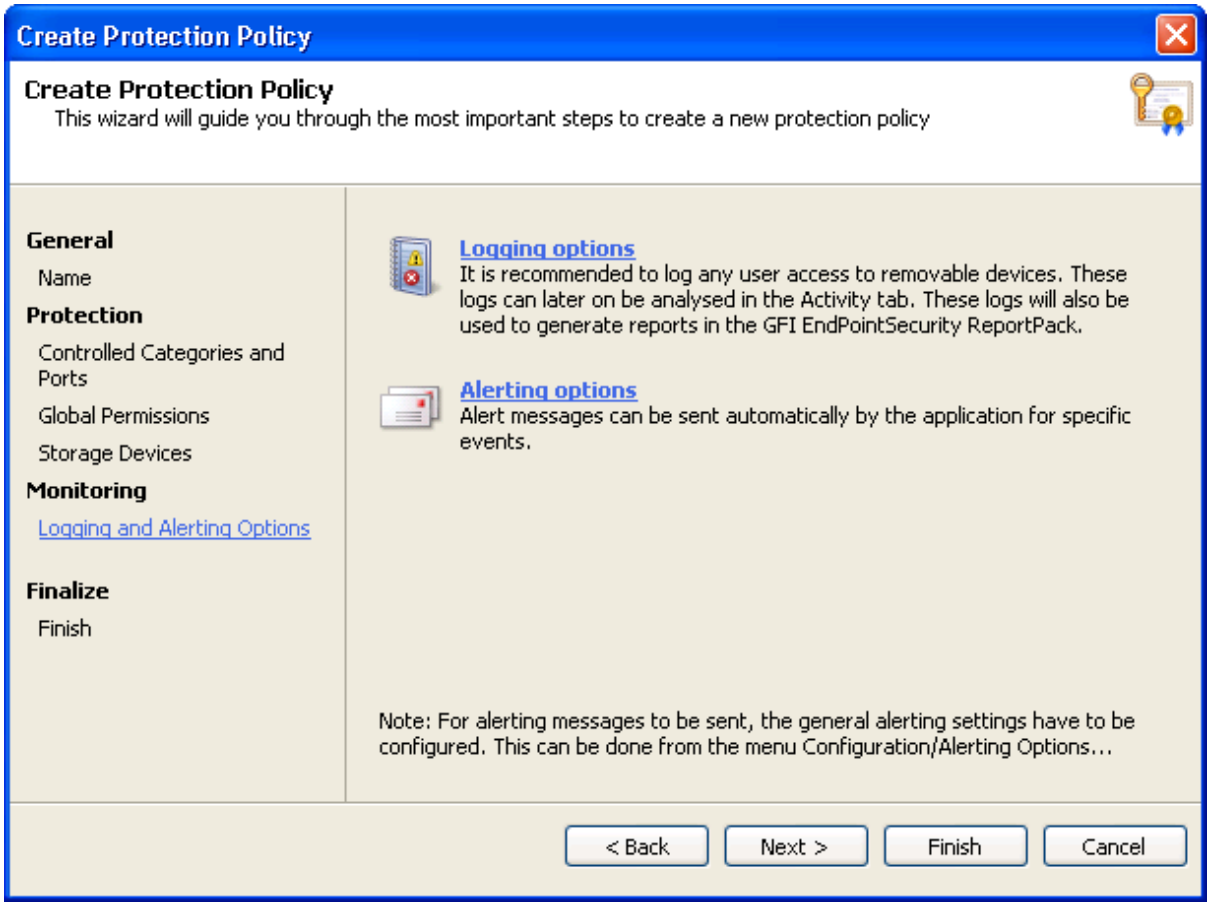
14. Click **OK** twice.

15. Click **Next**.

Step 6: Configuring logging and alerting options

GFI EndPointSecurity provides you with the facility to log device and port usage for analysis and report generation purposes. In addition, you can also configure the alert types to send to specified recipients when particular events are generated.

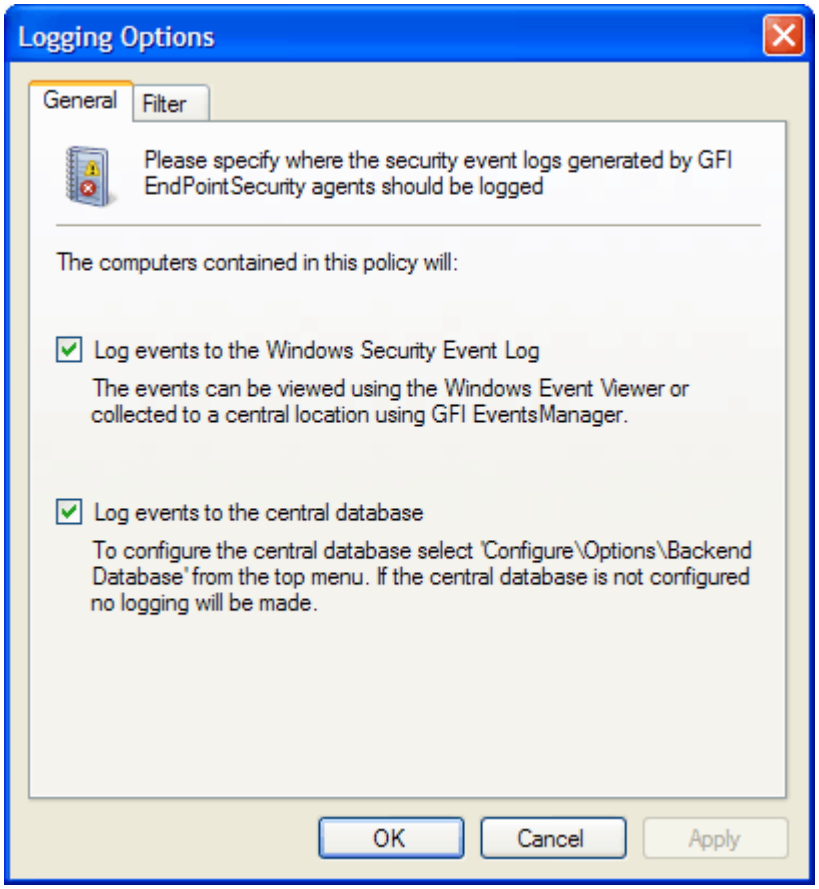
Alert recipients are not Active Directory (AD) users and/or user groups, or local users and/or groups schema, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts. It is best to create alert recipients prior to configuring alerts. For more information on how to create the users and groups for notification purposes, refer to the **Configuring alert recipients** section in the **Customizing GFI EndPointSecurity** chapter.


Create Protection Policy
Create Protection Policy
This wizard will guide you through the most important steps to create a new protection policy
General
Name
Protection
Controlled Categories and Ports
Global Permissions
Storage Devices
Monitoring
Logging and Alerting Options
Finalize
Finish
Logging options
It is recommended to log any user access to removable devices. These logs can later on be analysed in the Activity tab. These logs will also be used to generate reports in the GFI EndPointSecurity ReportPack.
Alerting options
Alert messages can be sent automatically by the application for specific events.
Note: For alerting messages to be sent, the general alerting settings have to be configured. This can be done from the menu Configuration/Alerting Options...
< Back
Next >
Finish
Cancel

Screenshot 13 - GFI EndPointSecurity Create Protection Policy wizard: Logging and Alerting Options step

To configure logging and alerting options for this protection policy:

1. Click the **Logging options** hyperlink.


Logging Options
General
Filter
Please specify where the security event logs generated by GFI EndPoint Security agents should be logged
The computers contained in this policy will:
Log events to the Windows Security Event Log
The events can be viewed using the Windows Event Viewer or collected to a central location using GFI EventsManager.
Log events to the central database
To configure the central database select 'Configure\Options\Backend Database' from the top menu. If the central database is not configured no logging will be made.
OK
Cancel
Apply

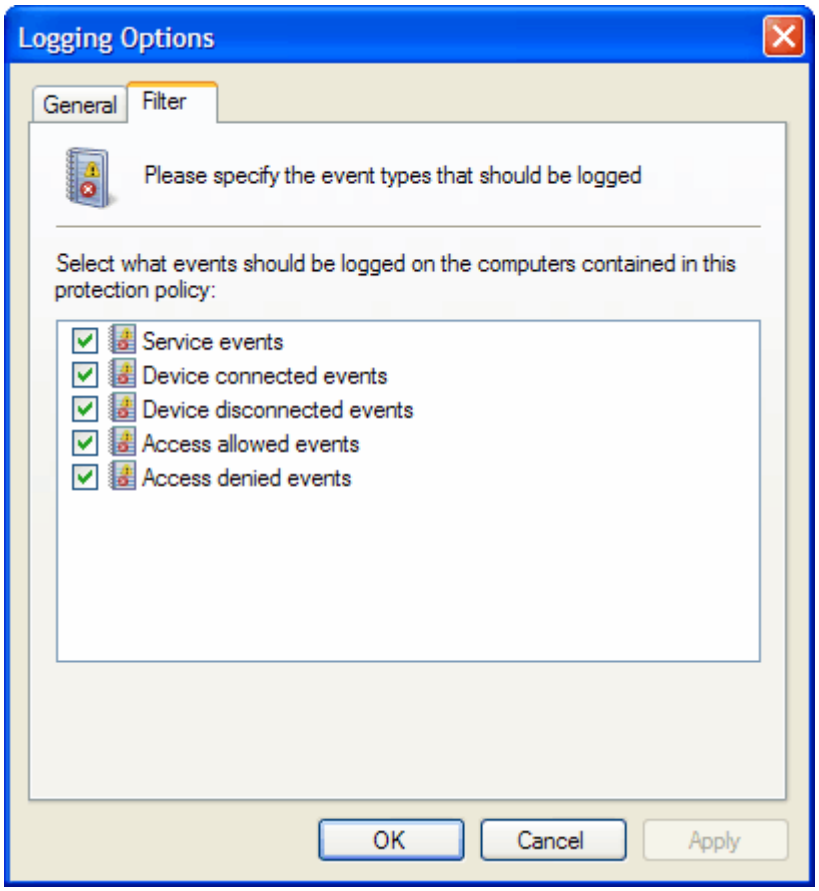
Screenshot 14 - Logging Options - General tab

2. In the **Logging Options** dialog select the **General** tab.

3. Enable or disable the locations where to store events generated by this protection policy:

   - **Log events to the Windows Security Event Log** - you can view events through the Windows Event Viewer of every target computer or through GFI EventsManager after they are collected in a central location.
   - **Log events to the central database** - you can view the events within the Logs Browser sub-tab in the GFI EndPointSecurity management console. This option requires the configuration of a central database. For more information on how to configure a central database, refer to the **Configuring database backend** section in the **Customizing GFI EndPointSecurity** chapter.

If both options are enabled, then the same data is logged in both locations.

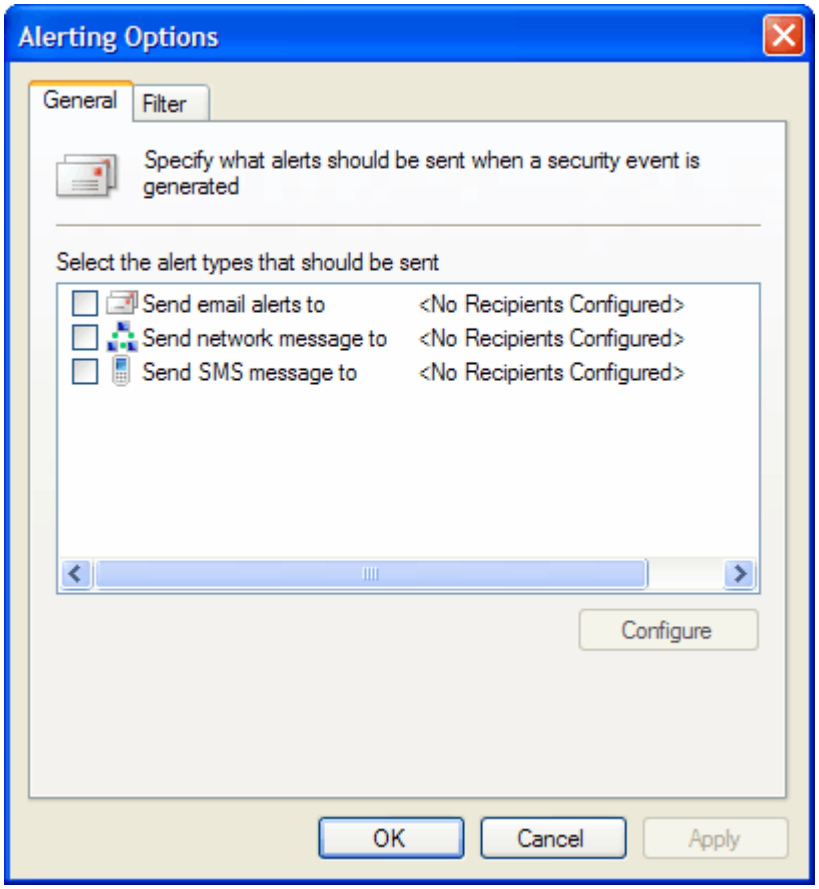


Screenshot 15 - Logging Options - Filter tab

4. Select the **Filter** tab, select any of the following event types that are to be logged by this protection policy and click **OK**:

- » Service events
- » Device connected events
- » Device disconnected events
- » Access allowed events
- » Access denied events.

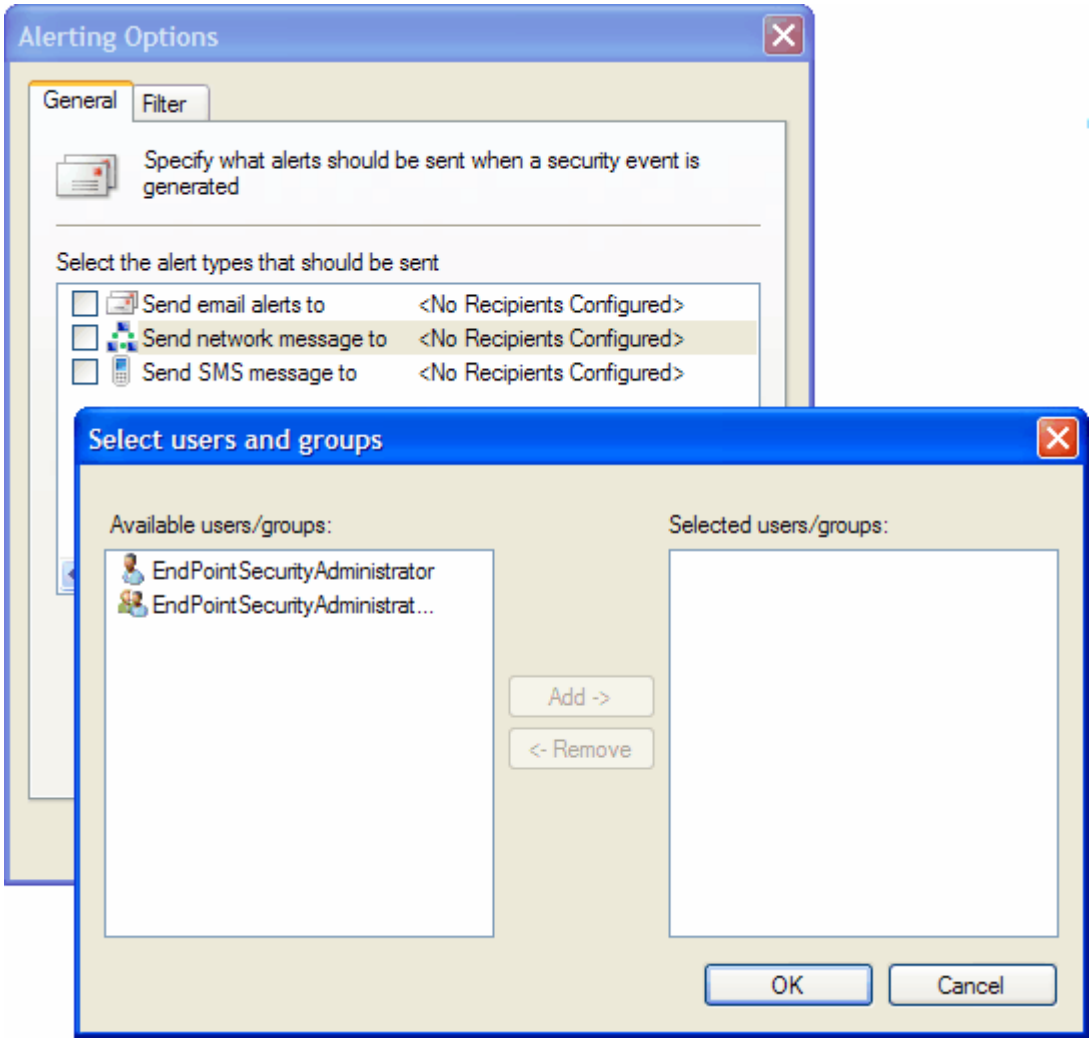
5. Click the **Alerting options** hyperlink.



Screenshot 16 - Alerting Options - General tab

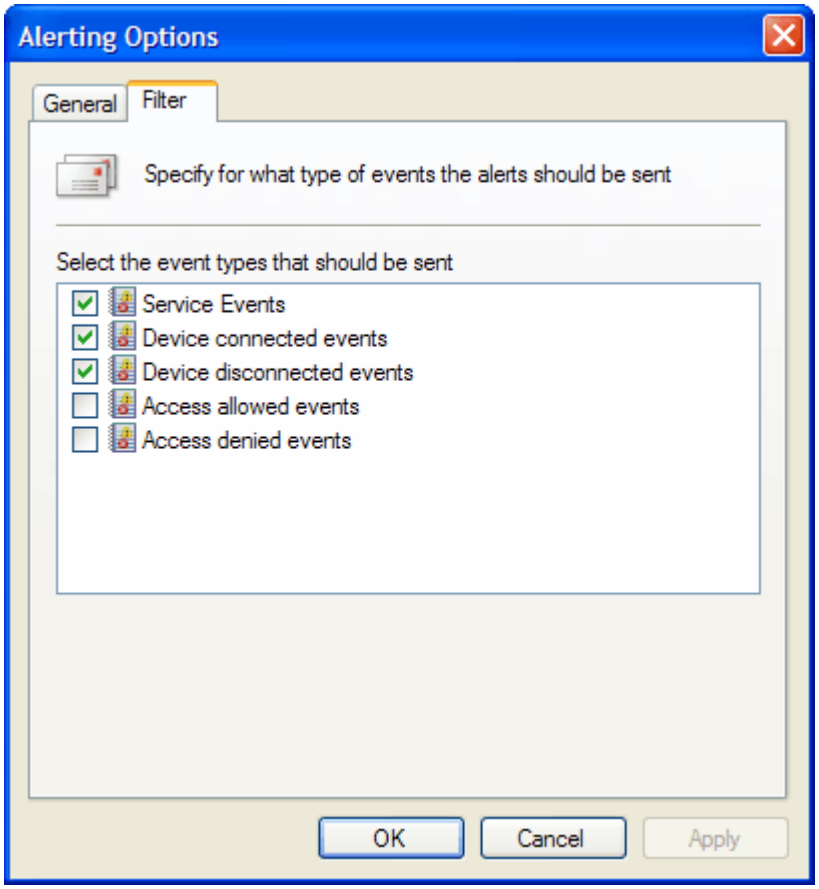
6. In the **Alerting Options** dialog, select the **General** tab and select any of the following alert types to be sent to alert recipients:

- Email alerts
- Network messages
- SMS messages.



Screenshot 17 - Alerting Options - Configuring users and groups

7. For each alert type enabled, highlight the alert type and click **Configure** to specify the user(s)/group(s) to whom the alert should be sent and click **OK**.



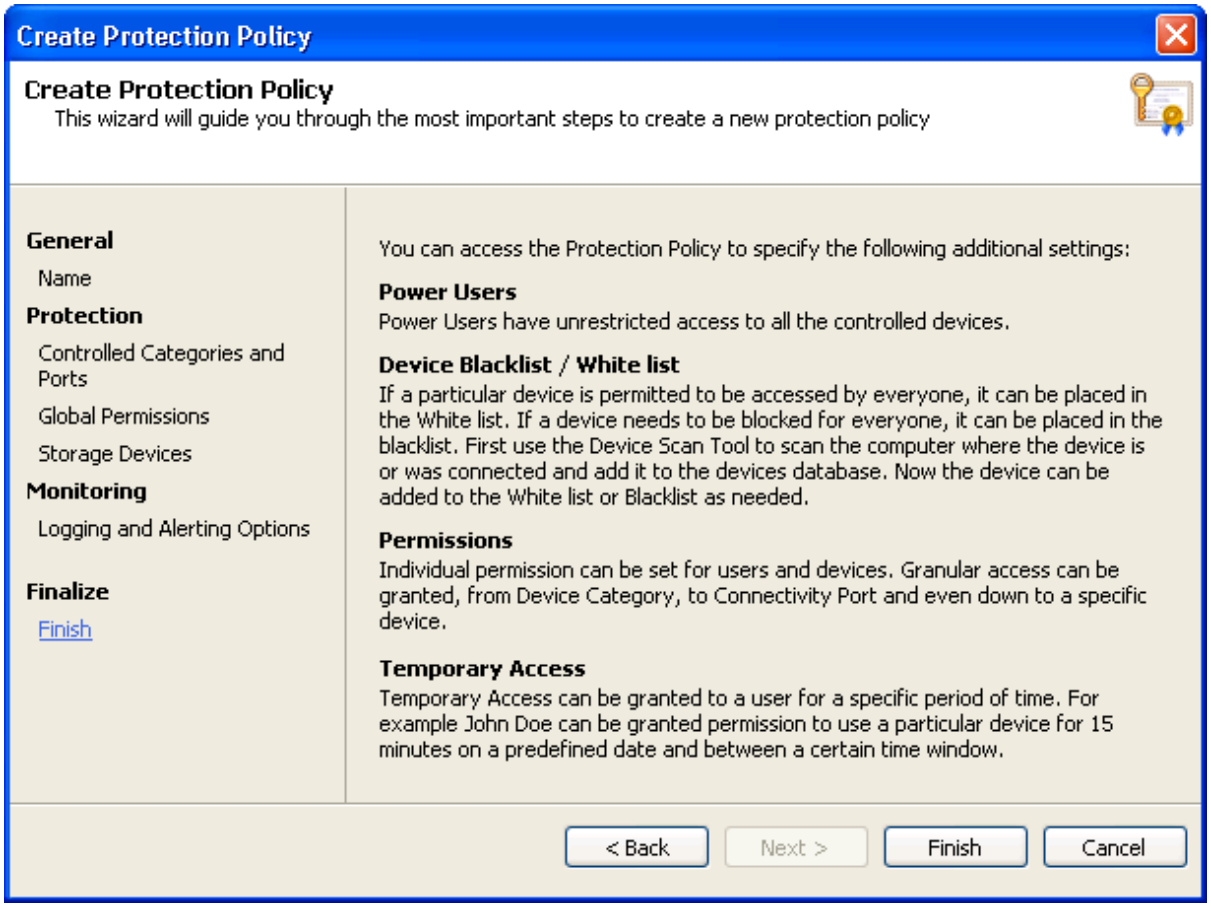
Screenshot 18 - Alerting Options - Filter tab

8. Select the **Filter** tab, select any of the following event types for which alerts are to be sent by this protection policy and click **OK**:

- » Service events
- » Device connected events
- » Device disconnected events
- » Access allowed events
- » Access denied events.

9. Click **Next**.

Step 7: Finalizing the wizard


Create Protection Policy
Create Protection Policy
This wizard will guide you through the most important steps to create a new protection policy
General
Name
Protection
Controlled Categories and Ports
Global Permissions
Storage Devices
Monitoring
Logging and Alerting Options
Finalize
Finish
You can access the Protection Policy to specify the following additional settings:
Power Users
Power Users have unrestricted access to all the controlled devices.
Device Blacklist / White list
If a particular device is permitted to be accessed by everyone, it can be placed in the White list. If a device needs to be blocked for everyone, it can be placed in the blacklist. First use the Device Scan Tool to scan the computer where the device is or was connected and add it to the devices database. Now the device can be added to the White list or Blacklist as needed.
Permissions
Individual permission can be set for users and devices. Granular access can be granted, from Device Category, to Connectivity Port and even down to a specific device.
Temporary Access
Temporary Access can be granted to a user for a specific period of time. For example John Doe can be granted permission to use a particular device for 15 minutes on a predefined date and between a certain time window.
< Back
Next >
Finish
Cancel

Screenshot 19 - GFI EndPointSecurity Create Protection Policy wizard: Finish step

To finalize the wizard for this protection policy:

1. Review the guidelines page.
2. Click Finish to complete the wizard.

4 Deploying protection policies

4.1 Introduction

Following the creation of a new protection policy, you need to deploy it on to target computers. In this chapter you will learn how to:

- Add a target computer in the computers list
- Assign a protection policy on to the target computer
- Deploy a protection policy on to the target computer
- Verify the deployment of a protection policy on to the target computer

Prior to deployment you can also modify the settings of your protection policy. For more information on how to configure specific settings, refer to the **Customizing protection policies** chapter in this manual.

4.2 Adding a target computer in the computers list

GFI EndPointSecurity provides you with the facility to specify the computers you intend to deploy agents and protection policies to (target computers). You can add target computers within the **Computers** list by:

- Adding it manually within the list
- Using the auto discovery feature.

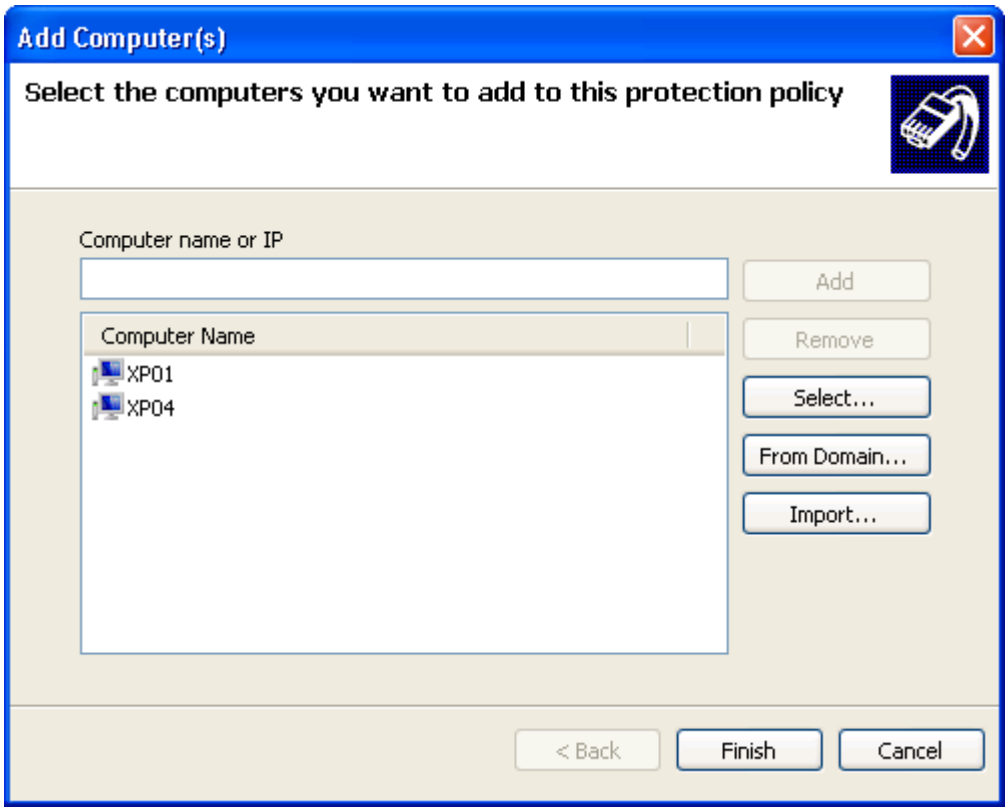
This section describes how to manually include a target computer within the Computers list.

For more information on how to automatically discover target computers and add them to the Computers list, refer to the **Configuring auto discovery settings** section in the **Customizing GFI EndPointSecurity** chapter.

4.2.1 Adding a target computer

To manually add a target computer in the Computers list:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Computers** sub-tab.
3. From the left pane, click the **Add computer(s)...** hyperlink in the **Common tasks** section.

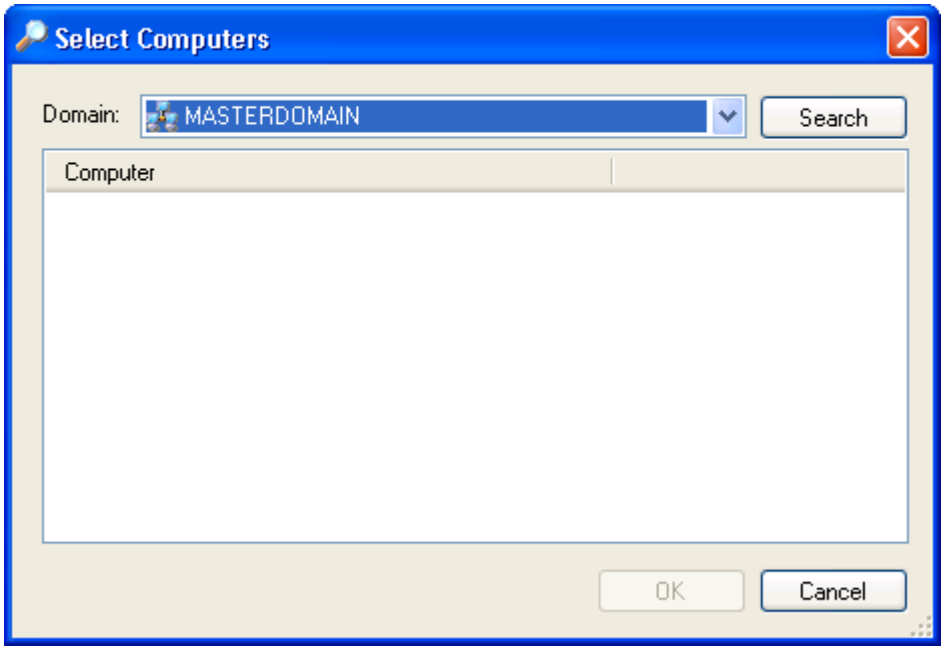


Screenshot 20 - Add Computer(s) options

4. In the **Add Computer(s)** dialog:

   » Option 1: Key in the name/IP of the target computer to add and click **Add**.

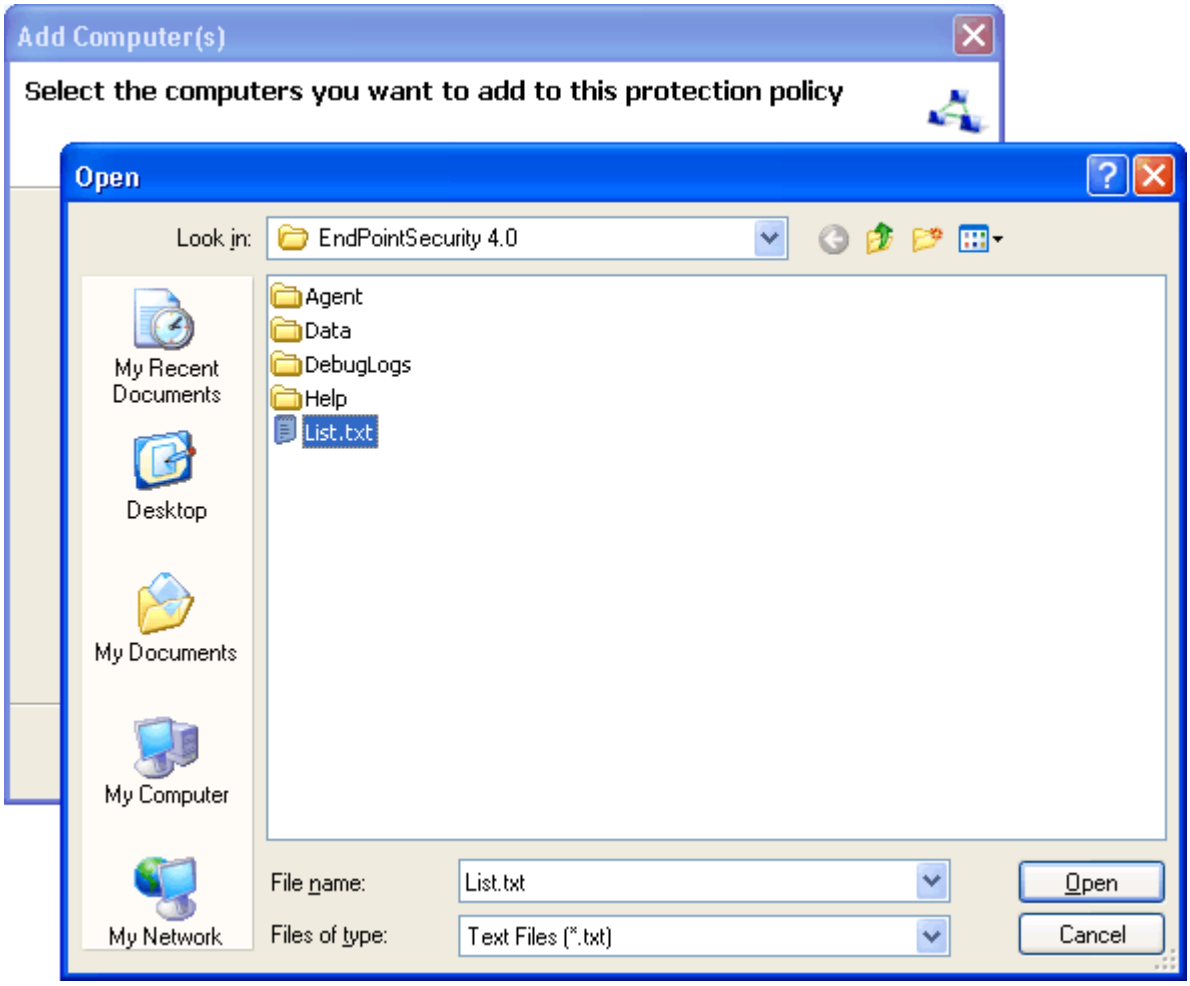
   Repeat the preceding sub-step for each target computer you want to add to this protection policy.



Screenshot 21 - Select Computers options

   » Option 2: Click **Select…**. In the **Select Computers** dialog select the relevant **Domain** from the drop-down list and click **Search**. Enable the required computer(s) and click **OK**.

   » Option 3: Click **From Domain…**. Specify the required computer(s) from within the domain where the GFI EndPointSecurity management console resides.



Screenshot 22 - Import computers options

» Option 4: Click **Import…**. Browse to the location of the text file that contains a list of computers to be imported.

5. Click **Finish**.

4.2.2 Configuring log on credentials

GFI EndPointSecurity requires to physically log on to the target computers in order to:

» Deploy agents and protection policy updates

» Keep track of the protection status of all target computers.

This requires that GFI EndPointSecurity is run under an account that has administrative privileges over your network target computers (e.g. a domain administrator account).

To specify logon credentials for a target computer:

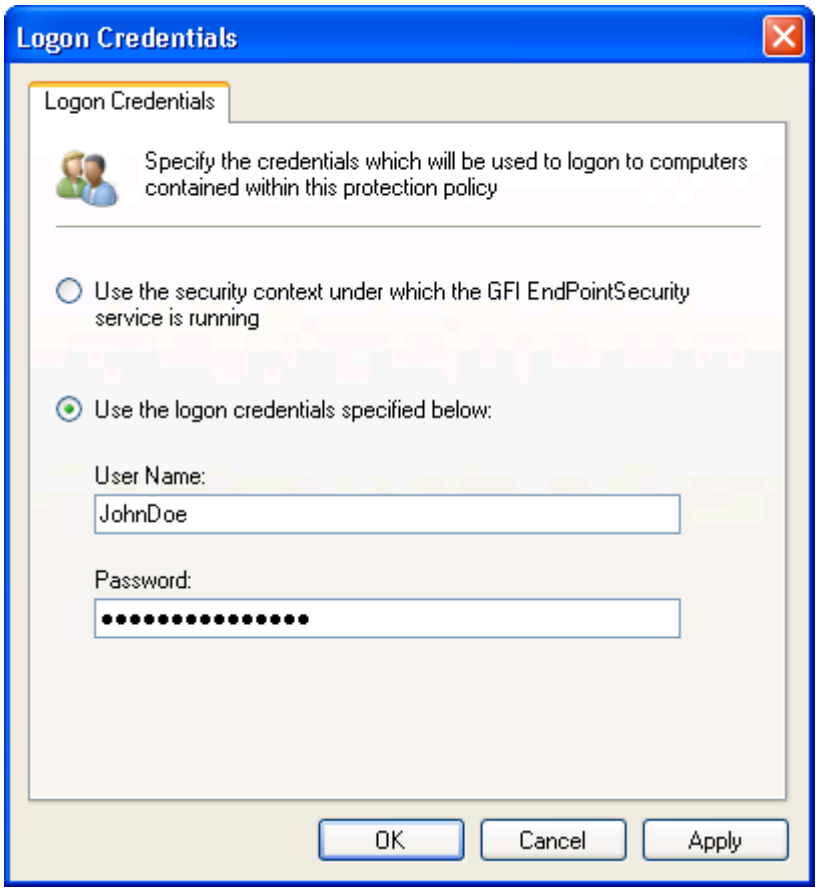
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. Highlight the required target computers.

If more than one target computer can be logged on in a similar way by GFI EndPointSecurity, you can highlight all the required target computers at once and then specify the logon credentials for the selected set of target computers.

4. From the left pane, click the **Set logon credentials…** hyperlink in the **Actions** section.


Logon Credentials
Logon Credentials
Specify the credentials which will be used to logon to computers contained within this protection policy
Use the security context under which the GFI EndPointSecurity service is running
Use the logon credentials specified below:
User Name:
JohnDoe
Password:
OK
Cancel
Apply

Screenshot 23 - Logon Credentials options

5. In the **Logon Credentials** dialog select the logon credentials that GFI EndPointSecurity requires to physically log on to the target computer(s), and click **OK**.

By default, GFI EndPointSecurity is configured to use the logon credentials of the currently logged-on user account from which GFI EndPointSecurity application is running.

4.3 Assigning a protection policy

Next step is to link the relevant set of device access and connectivity port permissions to each target computer. You can do this by assigning protection policies to target computers.

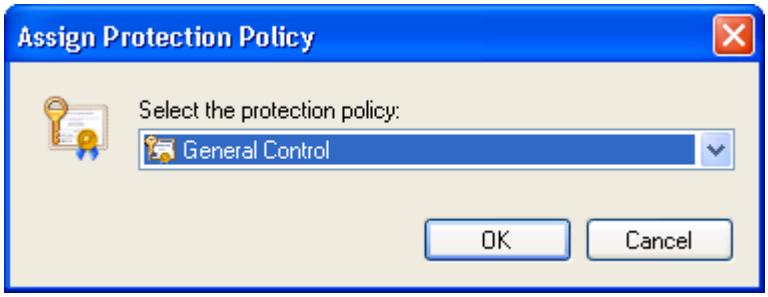
Target computers can only be assigned one protection policy at a time.

To assign a protection policy on to a target computer:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Computers** sub-tab.
3. Highlight the required target computer(s).

If the same policy is to be assigned to more than one target computer, you can highlight all the required target computers at once and then specify the protection policy for the selected set of target computers.

4. From the left pane, click the **Assign policy…** hyperlink in the **Actions** section.



Screenshot 24 - Assign Protection Policy options

5. In the **Assign Protection Policy** dialog select the required protection policy from the drop-down list, and click **OK**.

4.4 Deploying a protection policy

The final step is to apply the relevant set of device access and connectivity port permissions to each target computer. You can do this by deploying protection policies on to target computers using one of the following methods:

- Deploy immediately
- Schedule the deployment
- Deploy through Active Directory.

Upon the first deployment of a protection policy, a GFI EndPointSecurity agent is automatically installed on the remote network target computer. Upon the next deployments of the same protection policy, the agent will be updated and not re-installed.

4.4.1 Deploy immediately

To immediately deploy a protection policy on to a target computer:

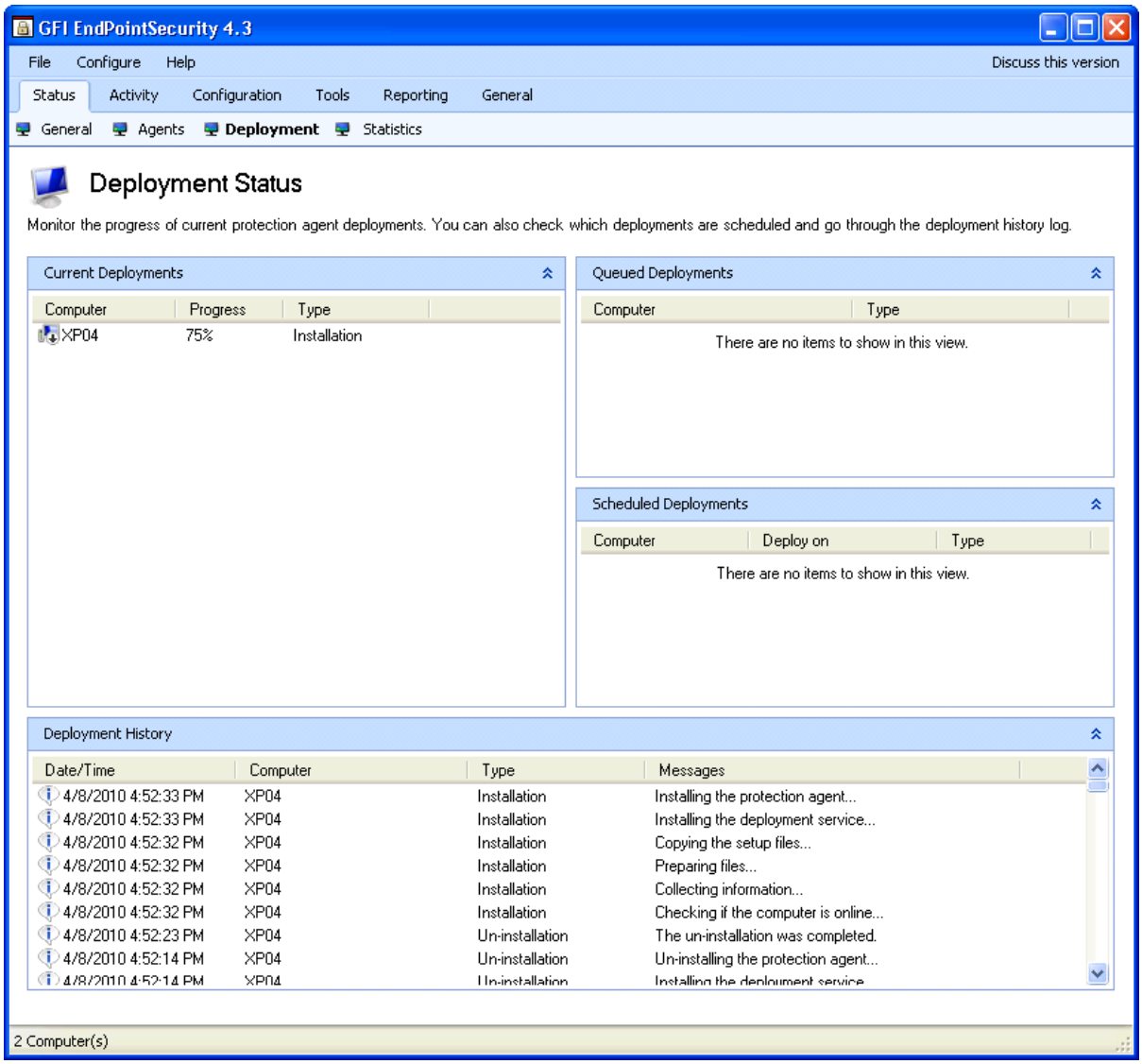
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. Highlight the required target computer(s).

If more than one deployment is required, you can highlight all the required target computers at once and then deploy the protection policies to the selected set of target computers.

4. From the left pane, click the **Deploy now…** hyperlink in the **Actions** section. The view should automatically change to **Status ► Deployment**.


GFI EndPointSecurity 4.3
File Configure Help
Discuss this version
Status Activity Configuration Tools Reporting General
General Agents Deployment Statistics
Deployment Status
Monitor the progress of current protection agent deployments. You can also check which deployments are scheduled and go through the deployment history log.
Current Deployments
Computer Progress Type
XP04 75% Installation
Queued Deployments
Computer Type
There are no items to show in this view.
Scheduled Deployments
Computer Deploy on Type
There are no items to show in this view.
Deployment History
Date/Time Computer Type Messages
4/8/2010 4:52:33 PM XP04 Installation Installing the protection agent...
4/8/2010 4:52:33 PM XP04 Installation Installing the deployment service...
4/8/2010 4:52:32 PM XP04 Installation Copying the setup files...
4/8/2010 4:52:32 PM XP04 Installation Preparing files...
4/8/2010 4:52:32 PM XP04 Installation Collecting information...
4/8/2010 4:52:32 PM XP04 Installation Checking if the computer is online...
4/8/2010 4:52:23 PM XP04 Un-installation The un-installation was completed.
4/8/2010 4:52:14 PM XP04 Un-installation Un-installing the protection agent...
2 Computer(s)

Screenshot 25 - Deployment sub-tab

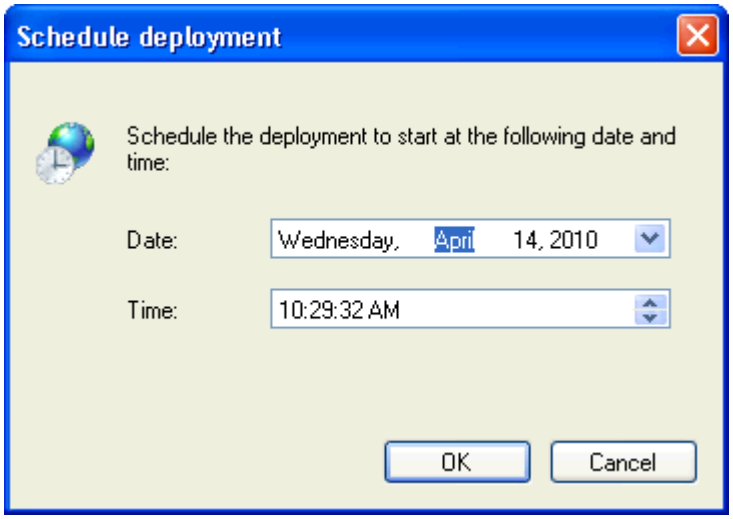
4.4.2 Schedule the deployment

To schedule deployment of a protection policy on to a target computer:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Computers** sub-tab.
3. Highlight the required target computer(s).

If more than one deployment is required, you can highlight all the required target computers at once and then deploy the policies to the selected set of target computers.

4. From the left pane, click the **Schedule deployment…** hyperlink in the **Actions** section.



Screenshot 26 - Schedule deployment options

5. In the **Schedule deployment** dialog select the deployment date and time, and click **OK**.

If the target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecurity keeps trying to deploy that policy every hour, until the target computer is back online.

4.4.3 Deploy through Active Directory

You can create a Windows installer package (.msi installation file) that you can then deploy through Active Directory Group Policies across target computers in your domain.

To create the Windows installer package:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy for which you want to create the Windows installer package.

4. From the right pane, click the **Deploy through Active Directory** hyperlink in the **Deployment** section.

5. Key in the **File name** of the .msi file and browse to select the destination path, and click **Save**.

For information on how to deploy software using Active Directory Group Policies in Microsoft Windows Server 2003 and Microsoft Windows Server 2008, refer to http://support.microsoft.com/kb/816102.

4.5 Verifying the deployment of a protection policy

Once the deployment of the protection policy is complete, it is recommended that you verify the success of the deployment, and to confirm the assignment of the correct protection policy to the target computers.

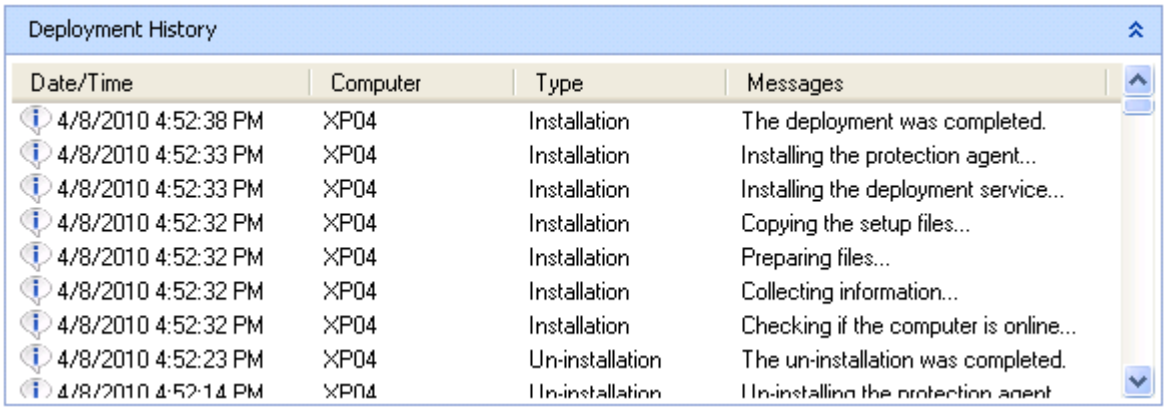
4.5.1 Deployment history

Use the information displayed in the **Deployment History** area to determine whether deployment for each target computer completed successfully, or whether errors were encountered.

To view the deployment history:

1. From the GFI EndPointSecurity management console, click on the **Status** tab.

2. Click on the **Deployment** sub-tab.


Deployment History
Date/Time
Computer
Type
Messages
4/8/2010 4:52:38 PM XP04 Installation The deployment was completed.
4/8/2010 4:52:33 PM XP04 Installation Installing the protection agent...
4/8/2010 4:52:33 PM XP04 Installation Installing the deployment service...
4/8/2010 4:52:32 PM XP04 Installation Copying the setup files...
4/8/2010 4:52:32 PM XP04 Installation Preparing files...
4/8/2010 4:52:32 PM XP04 Installation Collecting information...
4/8/2010 4:52:32 PM XP04 Installation Checking if the computer is online...
4/8/2010 4:52:23 PM XP04 Un-installation The un-installation was completed.

Screenshot 27 - Deployment History area

3. From the **Deployment History** area, confirm the successful completion of the update onto the local computer.

For more information about the deployment history area, refer to the **Deployment History** section in the **Monitoring statuses** chapter.

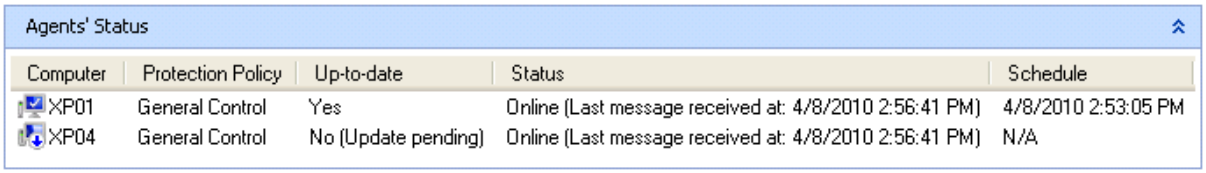
4.5.2 Agents' status

Use the information displayed in the **Agents' Status** area to determine the status of all deployment operations performed on your network target computers.

To view agents' status:

1. From the GFI EndPointSecurity management console, click on the **Status** tab.

2. Click on the **Agents** sub-tab.


Agents' Status
Computer
Protection Policy
Up-to-date
Status
Schedule
XP01 General Control Yes Online (Last message received at: 4/8/2010 2:56:41 PM) 4/8/2010 2:53:05 PM
XP04 General Control No (Update pending) Online (Last message received at: 4/8/2010 2:56:41 PM) N/A

Screenshot 28 - Agent's Status area

3. From the **Agents' Status** area, confirm the successful assignment of the correct protection policy to the target computer(s) and that agent deployment is up-to-date.

NOTE 1: Each agent sends its online status to the main GFI EndPointSecurity installation at regular intervals. If this data is not received by the main installation, the agent is considered to be offline.

NOTE 2: If a target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecurity keeps trying to deploy that policy every hour, until the target computer is back online.

For more information about the agents status area, refer to the **Agents sub-tab** section in the **Monitoring statuses** chapter.

5 Monitoring device usage activity

5.1 Introduction

GFI EndPointSecurity provides you with the facility to keep an audit trail of all events generated by GFI EndPointSecurity agents deployed on network computers. You can do this through:

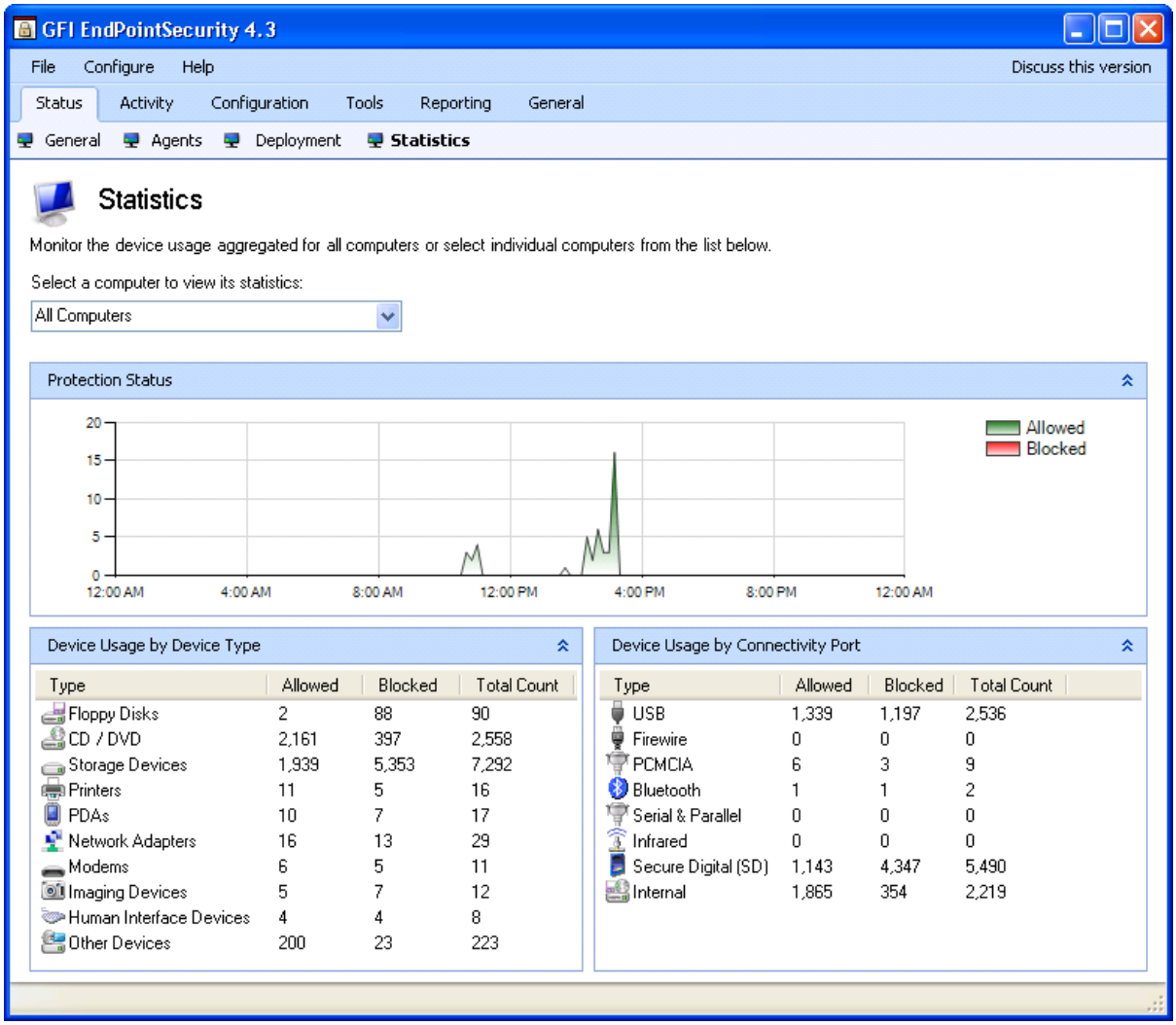
- The Statistics sub-tab
- The Activity tab.

NOTE 1: No content is displayed within these sub-tabs, if no database backend is configured. For more information on how to configure a central database, refer to the **Configuring database backend** section in the **Customizing GFI EndPointSecurity** chapter.

NOTE 2: To maintain an audit trail, you must enable logging. For information on how to enable logging, refer to the **Configuring event logging** section in the **Customizing protection policies** chapter.

5.2 Statistics

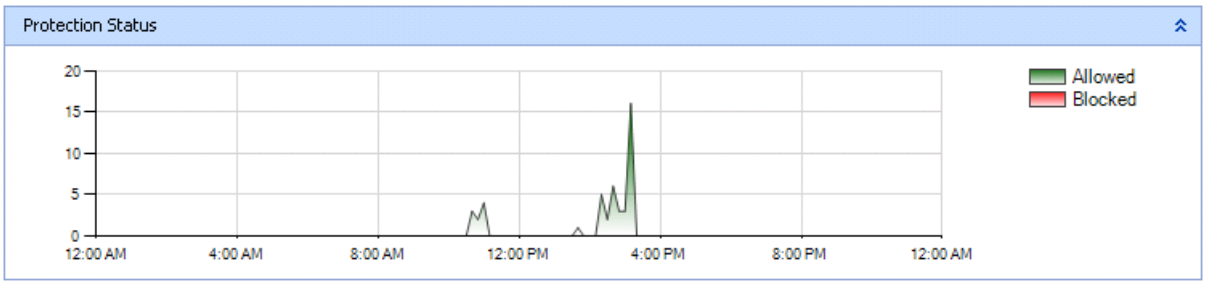
Use the **Statistics** sub-tab to view the daily device activity trends and statistics for a specific computer or for all network computers.



Screenshot 29 - Statistics sub-tab

To access the **Statistics** sub-tab, from the GFI EndPointSecurity management console click **Status** tab ► **Statistics**.

5.2.1 Protection Status



Screenshot 30 - Protection Status area

This section graphically represents daily device usage on computers, differentiating between devices that have been blocked and devices that have been allowed by the agents. The information provided can be filtered for a specific computer or for all network computers.

5.2.2 Device Usage by Device Type

Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Screenshot 31 - Device Usage by Device Type area

This section enumerates device connection attempts by device type, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

5.2.3 Device Usage by Connectivity Port

Device Usage by Connectivity Port

Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Screenshot 32 - Device Usage by Connectivity Port area

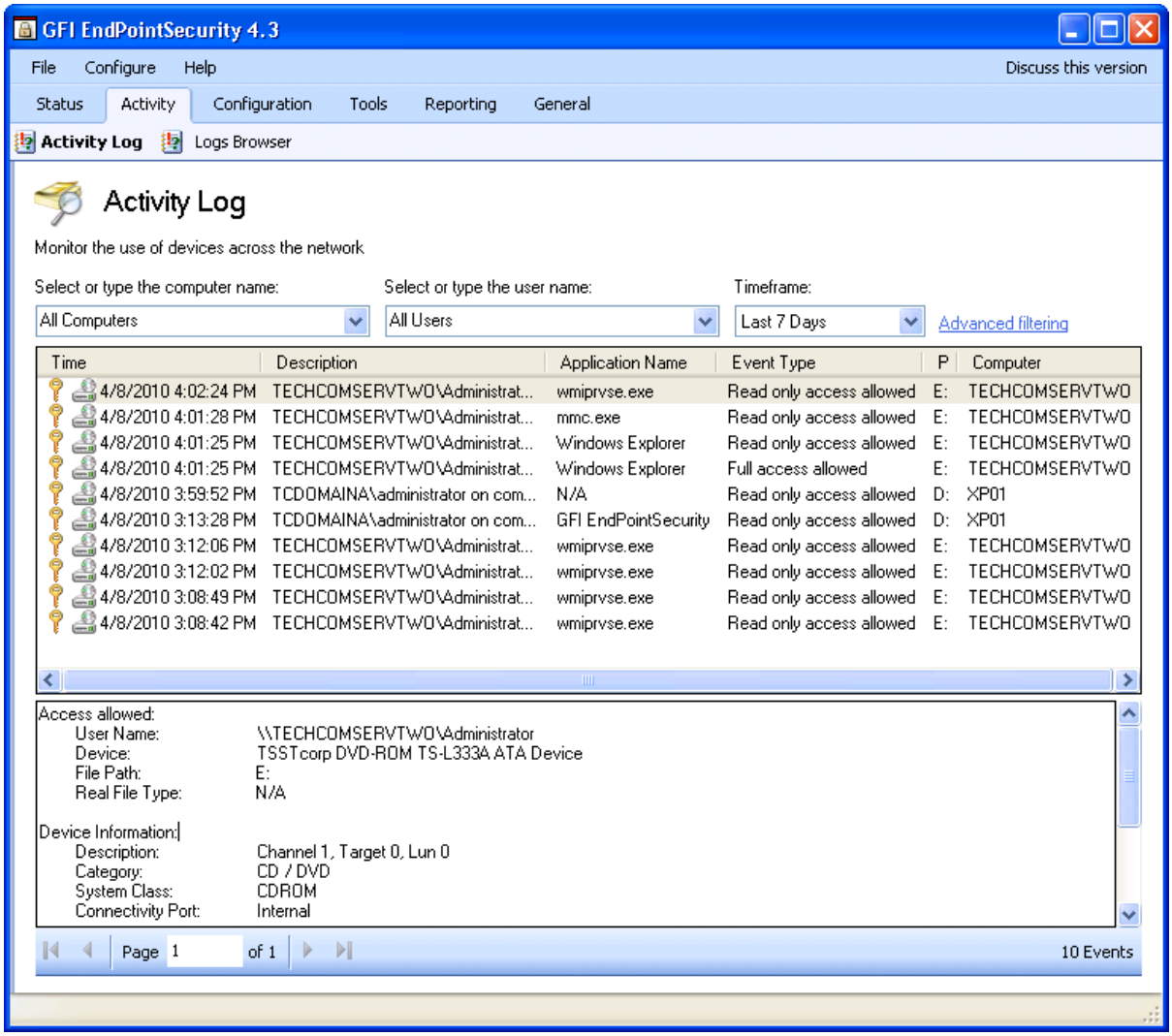
This section enumerates device connection attempts by connectivity port, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

5.3 Activity

Use the **Activity** tab to monitor device usage across the network and logged events for a specific computer or for all network computers.

5.3.1 Activity Log

This sub-tab allows you to monitor the devices in use on the network. Select the computer and/or user from the relevant dropdown lists to filter the Activity Log list by computer and/or by user. In addition, this tab allows you to further filter down the list by the provided time filters.


GFI EndPointSecurity 4.3
File
Configure
Help
Discuss this version
Status
Activity
Configuration
Tools
Reporting
General
Activity Log
Logs Browser
Activity Log
Monitor the use of devices across the network
Select or type the computer name:
Select or type the user name:
Timeframe:
All Computers
All Users
Last 7 Days
Advanced filtering
Time
Description
Application Name
Event Type
P
Computer
4/8/2010 4:02:24 PM TECHCOMSERVTWO\Administrat... wmiprvse.exe Read only access allowed E: TECHCOMSERVTWO
4/8/2010 4:01:28 PM TECHCOMSERVTWO\Administrat... mmc.exe Read only access allowed E: TECHCOMSERVTWO
4/8/2010 4:01:25 PM TECHCOMSERVTWO\Administrat... Windows Explorer Read only access allowed E: TECHCOMSERVTWO
4/8/2010 4:01:25 PM TECHCOMSERVTWO\Administrat... Windows Explorer Full access allowed E: TECHCOMSERVTWO
4/8/2010 3:59:52 PM TCDOMAINA\administrator on com... N/A Read only access allowed D: XP01
4/8/2010 3:13:28 PM TCDOMAINA\administrator on com... GFI EndPointSecurity Read only access allowed D: XP01
4/8/2010 3:12:06 PM TECHCOMSERVTWO\Administrat... wmiprvse.exe Read only access allowed E: TECHCOMSERVTWO
4/8/2010 3:12:02 PM TECHCOMSERVTWO\Administrat... wmiprvse.exe Read only access allowed E: TECHCOMSERVTWO
4/8/2010 3:08:49 PM TECHCOMSERVTWO\Administrat... wmiprvse.exe Read only access allowed E: TECHCOMSERVTWO
4/8/2010 3:08:42 PM TECHCOMSERVTWO\Administrat... wmiprvse.exe Read only access allowed E: TECHCOMSERVTWO
Access allowed:
User Name: \\TECHCOMSERVTWO\Administrator
Device: TSSTcorp DVD-ROM TS-L333A ATA Device
File Path: E:
Real File Type: N/A
Device Information:
Description: Channel 1, Target 0, Lun 0
Category: CD / DVD
System Class: CDROM
Connectivity Port: Internal
Page 1 of 1
10 Events

Screenshot 33 - Activity Log sub-tab

To access the **Activity Log** sub-tab, from the GFI EndPointSecurity management console click **Activity** tab ► **Activity Log**.

To view more details about a particular event click on the event. Additional information is displayed in the events description pane at the bottom of the sub-tab.

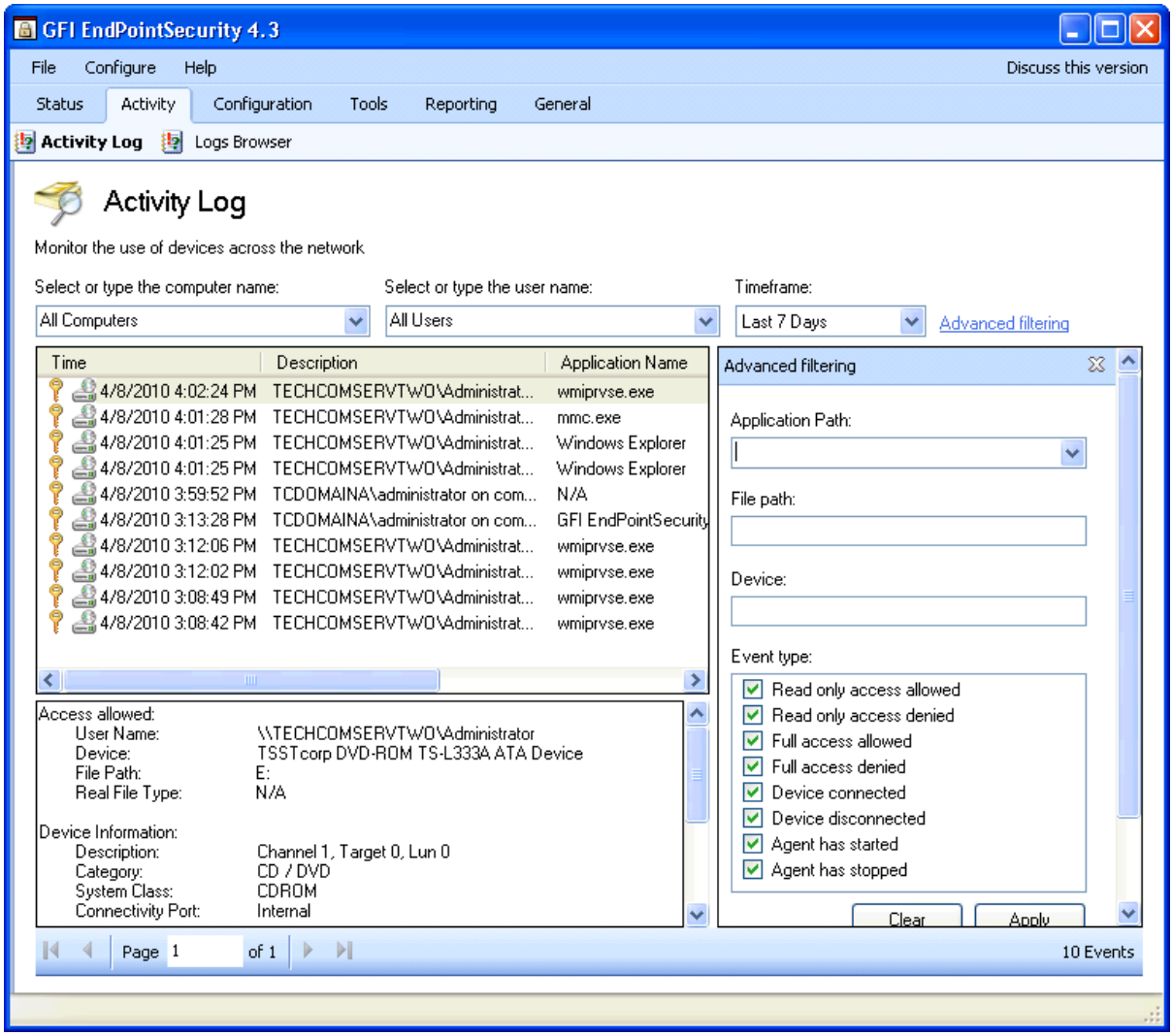
To customize the **Activity Log** sub-tab to suit your company's needs, right-click the header and select the columns that should be added to or removed from the view.

To change a column's position, select the column header, drag and drop it at the required position.

Advanced Filtering

This feature allows you to further filter down the device usage history logs using one or more criteria from the following set:

- Application Path
- File path
- Device
- Event type



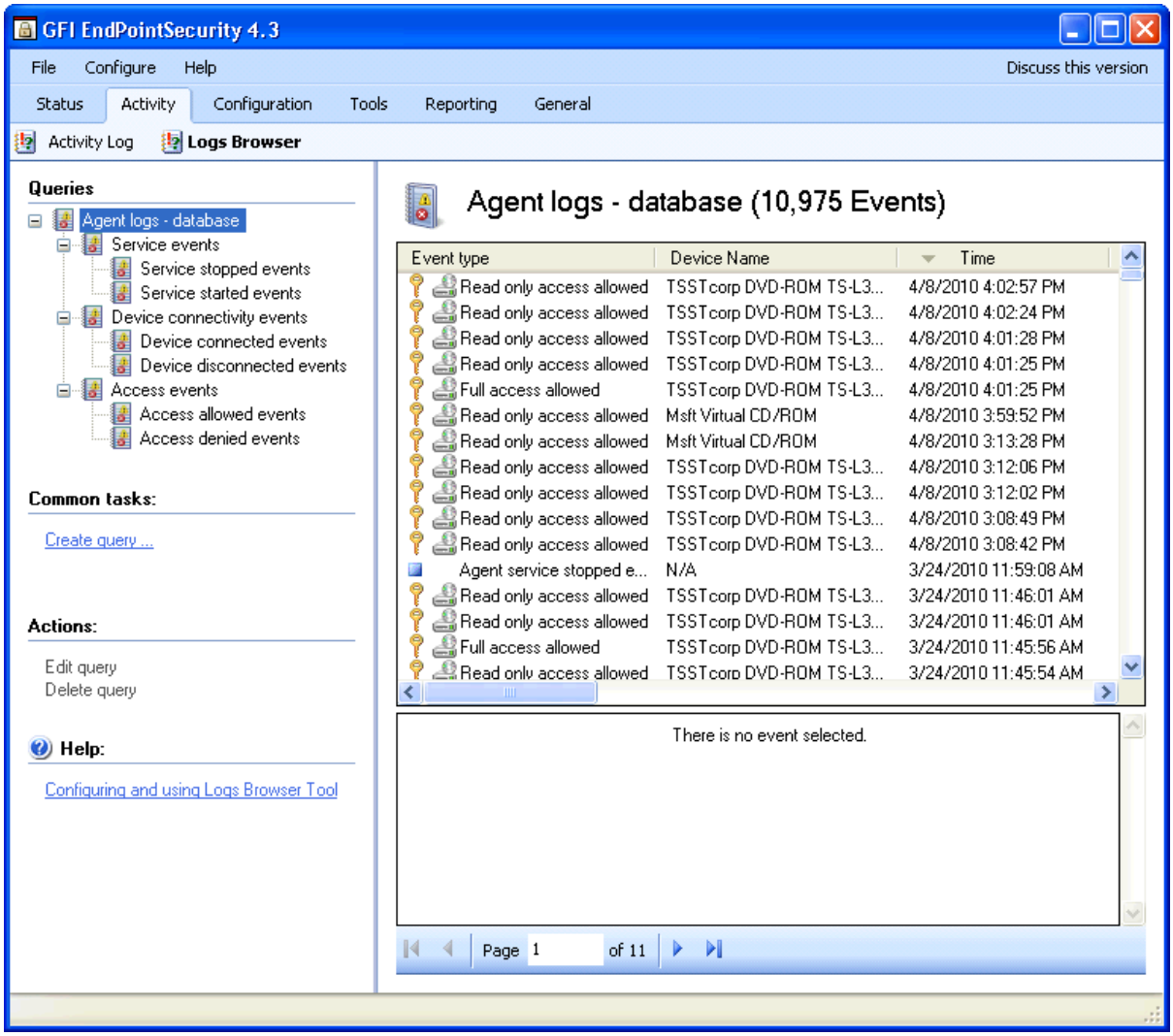
Screenshot 34 - Activity Log sub-tab - Advanced filtering

To access the advanced filtering of the Activity Log, click the Advanced filtering hyperlink in the **Activity Log** sub-tab.

5.3.2 Logs Browser

This sub-tab allows you to access and browse events currently stored in the database backend.

GFI EndPointSecurity also includes a query builder to simplify searching for specific events. With the events query builder you can create custom filters that filter events data and display only the information that you need to browse - without deleting one single record from your database backend.


GFI EndPointSecurity 4.3
File
Configure
Help
Discuss this version
Status
Activity
Configuration
Tools
Reporting
General
Activity Log
Logs Browser
Queries
Agent logs - database
Service events
Service stopped events
Service started events
Device connectivity events
Device connected events
Device disconnected events
Access events
Access allowed events
Access denied events
Common tasks:
Create query ...
Actions:
Edit query
Delete query
Help:
Configuring and using Logs Browser Tool
Agent logs - database (10,975 Events)
Event type
Device Name
Time
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 4:02:57 PM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 4:02:24 PM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 4:01:28 PM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 4:01:25 PM
Full access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 4:01:25 PM
Read only access allowed Msft Virtual CD/ROM 4/8/2010 3:59:52 PM
Read only access allowed Msft Virtual CD/ROM 4/8/2010 3:13:28 PM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 3:12:06 PM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 3:12:02 PM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 3:08:49 PM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 4/8/2010 3:08:42 PM
Agent service stopped e... N/A 3/24/2010 11:59:08 AM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 3/24/2010 11:46:01 AM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 3/24/2010 11:46:01 AM
Full access allowed TSSTcorp DVD-ROM TS-L3... 3/24/2010 11:45:56 AM
Read only access allowed TSSTcorp DVD-ROM TS-L3... 3/24/2010 11:45:54 AM
There is no event selected.
Page 1 of 11

Screenshot 35 - Logs Browser sub-tab

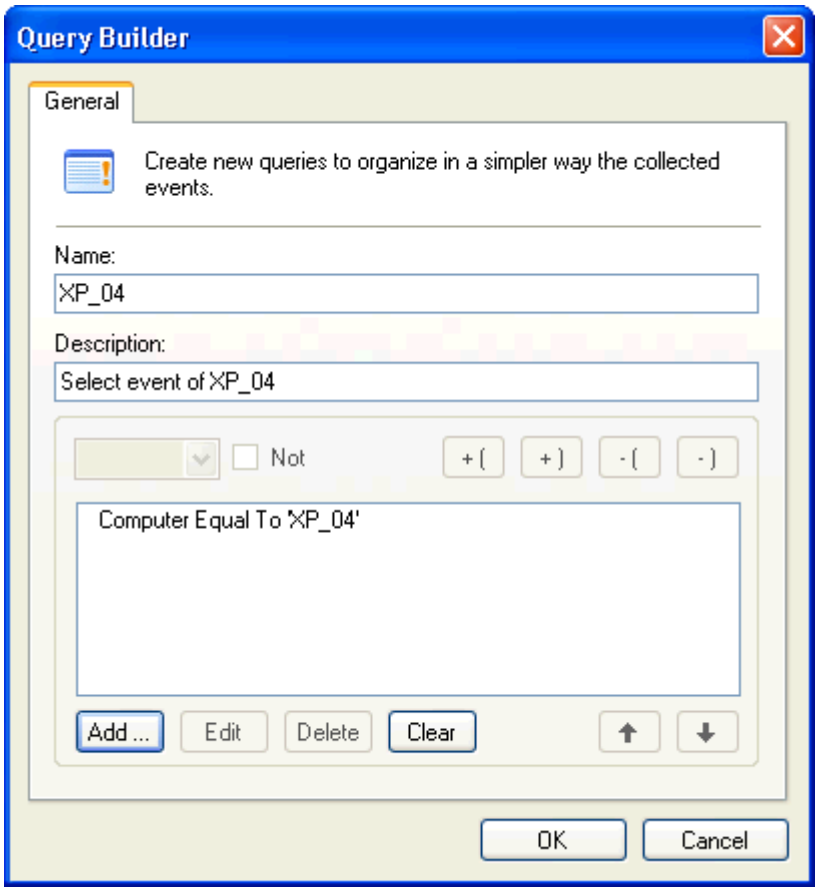
To access the **Logs Browser** sub-tab, from the GFI EndPointSecurity management console click **Activity** tab ► **Logs Browser**.

To view more details about a particular event, click on the event. Additional information is displayed in the events description pane at the bottom of the sub-tab.

Creating event queries

To create custom event queries:

1. From the GFI EndPointSecurity management console, click on the **Activity** tab.
2. Click on the **Logs Browser** sub-tab.
3. In the left pane, select **Agent logs - database** node.
4. Right-click and select **Create query…**



Screenshot 36 - Query Builder options

5. In the **Query Builder** dialog, specify a name and a description for the new query.

6. Click **Add…**, configure the required query condition(s) and click **OK**. Repeat until all required query conditions have been specified.

7. Click **OK** to finalize your settings. The custom query is added as a sub-node within **Agent logs - database** node.

You can also filter the results of existing event queries by creating more specific sub-queries. To do this right-click on the specific query and select **Create query…**.

6 Monitoring statuses

6.1 Introduction

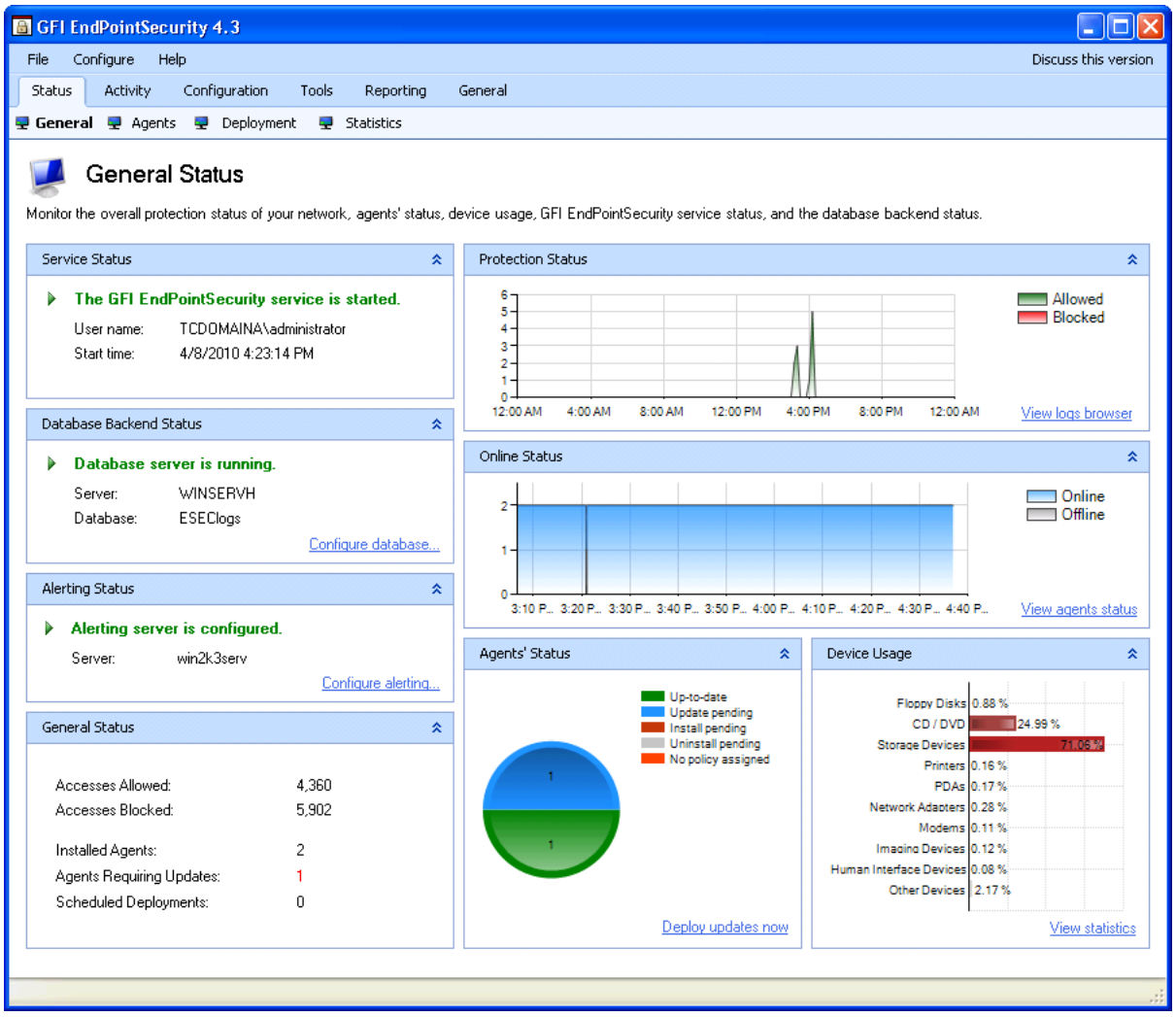
The status monitor is a dashboard that shows the status of GFI EndPointSecurity as well as the status of agents deployed on network computers. It also provides you with graphs and statistical information related to device usage. The status monitor consists of four different dashboard sub-tabs:

- General Status
- Agents Status
- Deployment Status
- Statistics.

6.2 General

Use the **General** sub-tab to view:

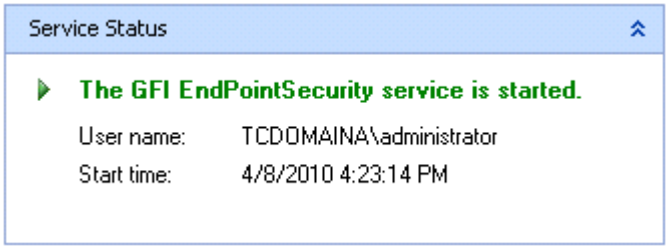
- The statuses of the GFI EndPointSecurity service, of the database backend server and of the alerting server
- The status of GFI EndPointSecurity agents deployed on network computers
- Device usage such as the number and percentage of devices blocked and the number of devices allowed.



Screenshot 37 - General sub-tab

To access the **General** sub-tab, from the GFI EndPointSecurity management console click **Status** tab ► **General**.

6.2.1 Service Status


Service Status
The GFI EndPointSecurity service is started.
User name: TCDOMAINA\administrator
Start time: 4/8/2010 4:23:14 PM

Screenshot 38 - Service Status area

This section lists:

- The operational status of the GFI EndPointSecurity management console service
- The user account under which the GFI EndPointSecurity service is running
- The time when the service was last started.

6.2.2 Database Backend Status

Screenshot 39 - Database Backend Status area

This section lists:

- The operational status of the database server currently in use by GFI EndPointSecurity
- The name or IP address of the database server currently in use by GFI EndPointSecurity
- The name of the database in which GFI EndPointSecurity is archiving events.

To modify any of the current database settings, click on the **Configure database…** hyperlink. This will launch the **Database Backend** dialog. For more information on how to configure a central database, refer to the **Configuring database backend** section in the **Customizing GFI EndPointSecurity** chapter.

6.2.3 Alerting Status

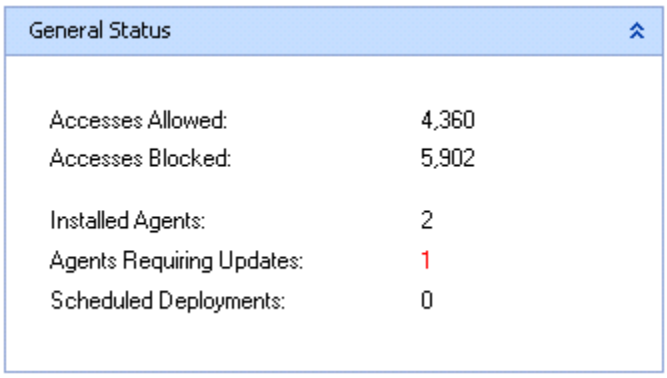
Screenshot 40 - Alerting Status area

This section lists:

- The operational status of the alerting server currently in use by GFI EndPointSecurity
- The name or IP address of the alerting server currently in use by GFI EndPointSecurity

To modify any of the current alerts related settings, click on the **Configure alerting …** hyperlink. This will launch the **Alerting Options** dialog. For more information, refer to the **Configuring alerting options** section in the **Customizing GFI EndPointSecurity** chapter.

6.2.4 General Status



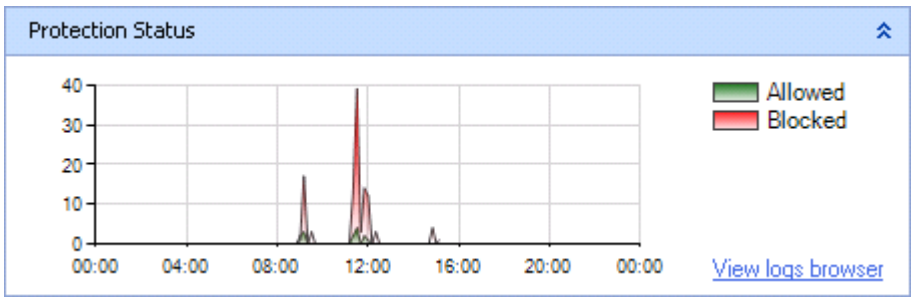
Screenshot 41 - General Status area

Access related values will be set as N/A and those related to agents will be set to zero within this area, if no database backend is configured. For more information on how to configure a central database, refer to the **Configuring database backend** section in the **Customizing GFI EndPointSecurity** chapter.

This section lists the cumulative values of the number of:

- User accesses to devices allowed by the agents
- User accesses to devices blocked by the agents
- Agents installed on network computers
- Agents that need to be updated, which include:
  - Agents to be installed
  - Agents to be uninstalled
  - Protection policy updates
- Scheduled deployments, which include:
  - Agents to be installed
  - Agents to be uninstalled
  - Protection policy updates

6.2.5 Protection Status



Screenshot 42 - Protection Status area

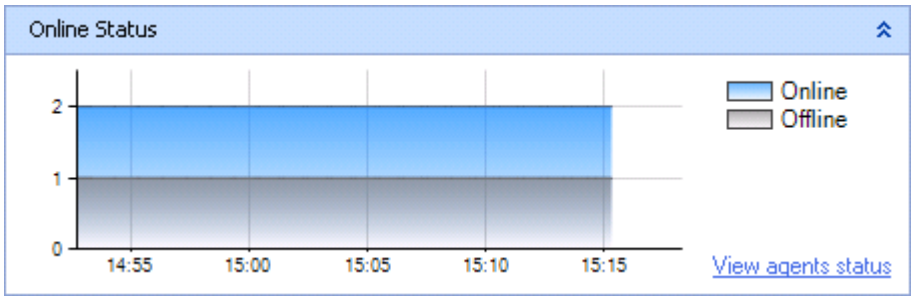
No content is displayed within this area, if no database backend is configured. For more information on how to configure a central database, refer to the **Configuring database backend** section in the **Customizing GFI EndPointSecurity** chapter.

This section graphically represents daily device usage on network computers, differentiating between devices that have been blocked and devices that have been allowed by the agents.

To view an in-depth analysis of events, including those for devices that have been blocked/allowed, click on the **View logs browser** hyperlink. This will launch the **Logs Browser**

sub-tab. For more information, refer to the **Logs Browser sub-tab** section in the **Monitoring device usage activity** chapter.

6.2.6 Online Status

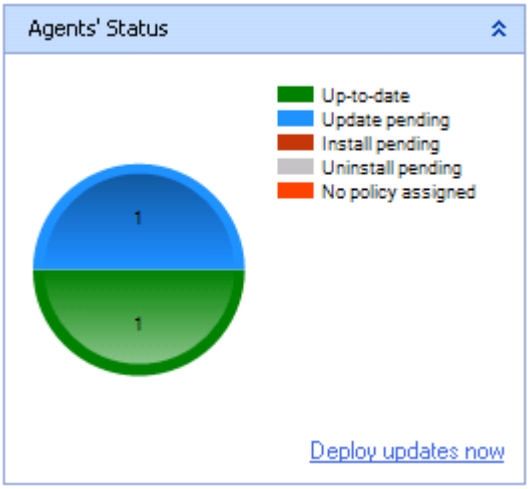


Screenshot 43 - Online Status area

This section graphically represents all agents deployed on network computers, differentiating between those that are currently online and those that are offline.

To view details of agents' statuses, click on the **View agents status** hyperlink. This will launch the **Agents** sub-tab. For more information, refer to the **Agents sub-tab** section in this chapter.

6.2.7 Agents' Status



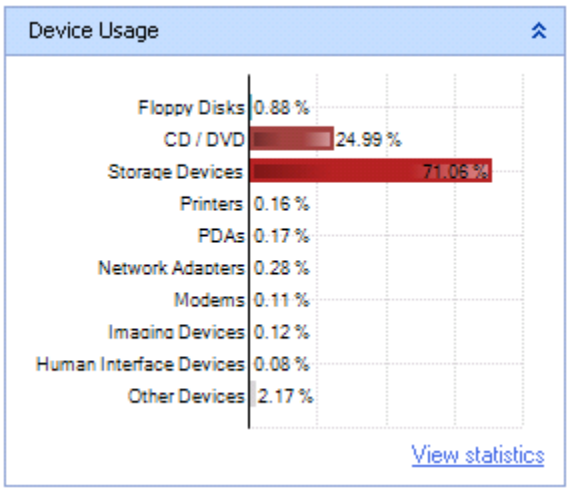
Screenshot 44 - Agents' Status area

This section graphically represents the number of agents that currently:

- Are deployed and in-sync with the protection policy
- Are deployed but need to be updated with protection policy changes
- Are awaiting installation on network computers
- Are awaiting un-installation from network computers
- Are not protected by a protection policy.

To install agents and deploy updates, click on the **Deploy updates now** hyperlink. This will launch the **Select computers for deployment** dialog, select the required target computers and click **OK**.

6.2.8 Device Usage



Screenshot 45 - Device Usage area

No content is displayed within this area, if no database backend is configured. For more information on how to configure a central database, refer to the **Configuring database backend** section in the **Customizing GFI EndPointSecurity** chapter.

This section graphically represents the percentages of user accesses per device category of the total cumulative amount of user accesses to devices, as logged by the agents. User accesses to devices refer to both allowed and blocked device accesses.

To view a statistical breakdown of device usage, showing the numbers of device types and connectivity ports that have been blocked or allowed for either a specific computer or for all network computers, click on the **View statistics** hyperlink. This will launch the **Statistics** sub-tab. For more information, refer to the **Statistics sub-tab** section in the **Monitoring device usage activity** chapter.

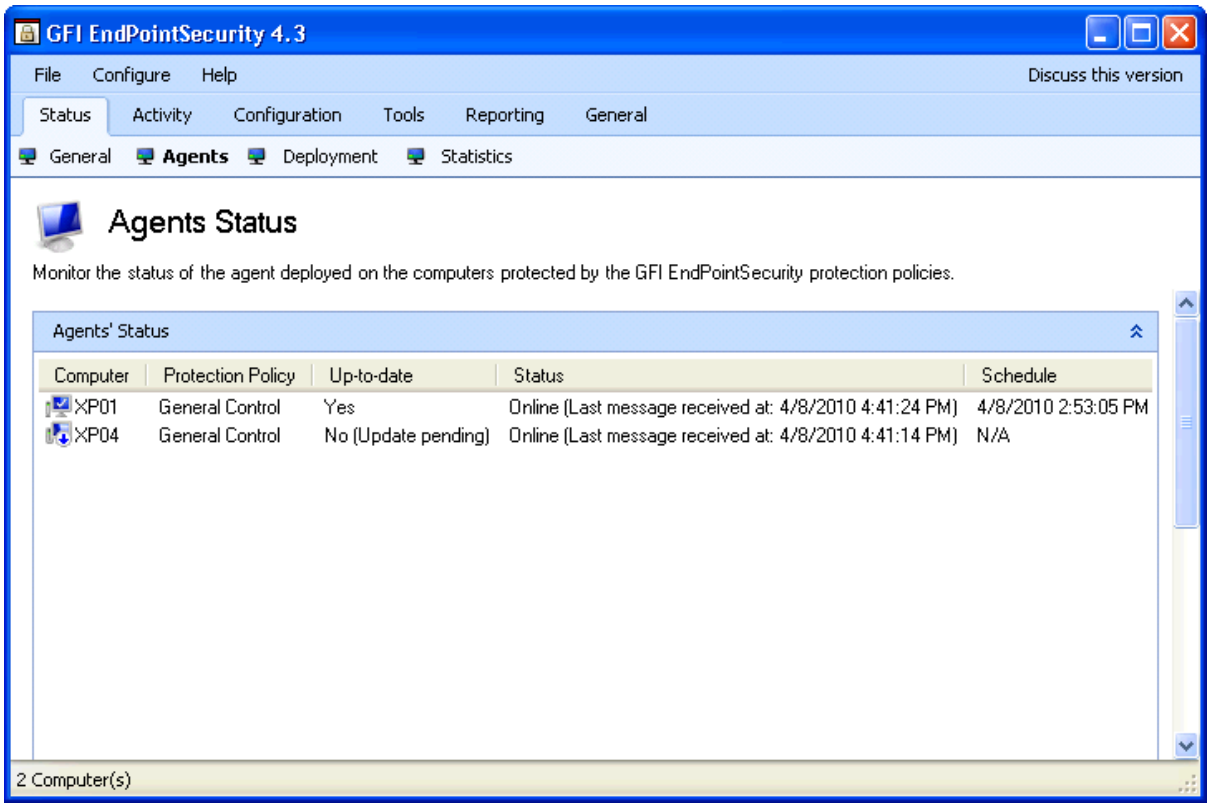
6.3 Agents

Use the **Agents** sub-tab to determine the status of all deployment operations performed on your network targets. For each target computer, information displayed shows:

- Target computer name and applicable protection policy
- The status of the GFI EndPointSecurity agent, whether currently deployed and up-to-date, or awaiting deployment
- The status of the target computer, whether currently online, or offline.

NOTE 1: If a target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecurity keeps trying to deploy that policy every hour, until the target computer is back online.

NOTE 2: Each agent sends its online status to the GFI EndPointSecurity application at regular intervals. If this data is not received by the main application, the agent is considered to be offline.



Screenshot 46 - Agents sub-tab

To access the **Agents** sub-tab, from the GFI EndPointSecurity management console click **Status** tab ► **Agents**.

To deploy pending agents:

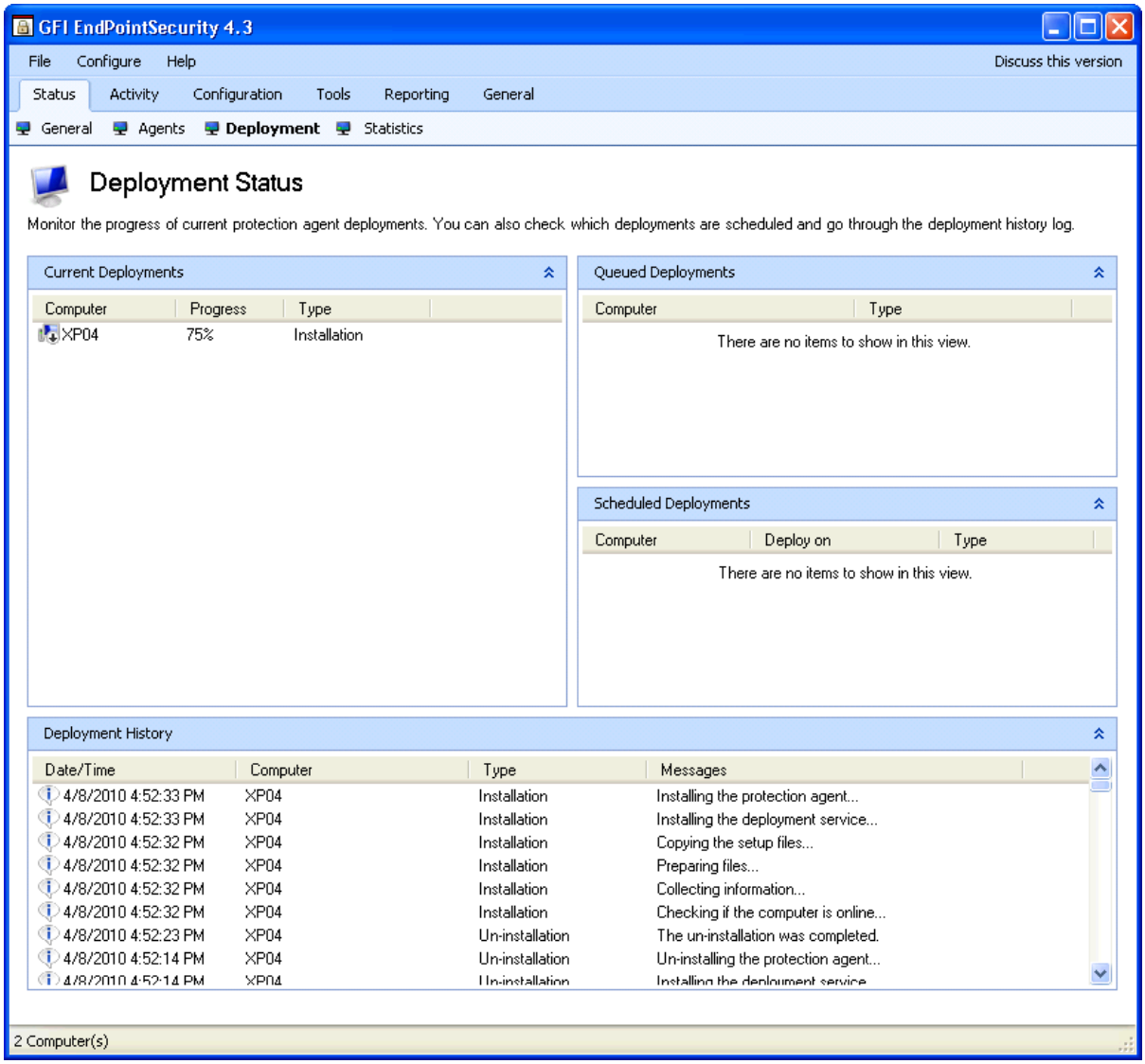
1. Select one or more computers from the **Agents' Status** section.

2. Right-click on the selected computers and select **Deploy selected agent(s)** or **Schedule deployment for selected agent(s)…**, and click **OK**.

6.4 Deployment

Use the **Deployment** sub-tab to view:

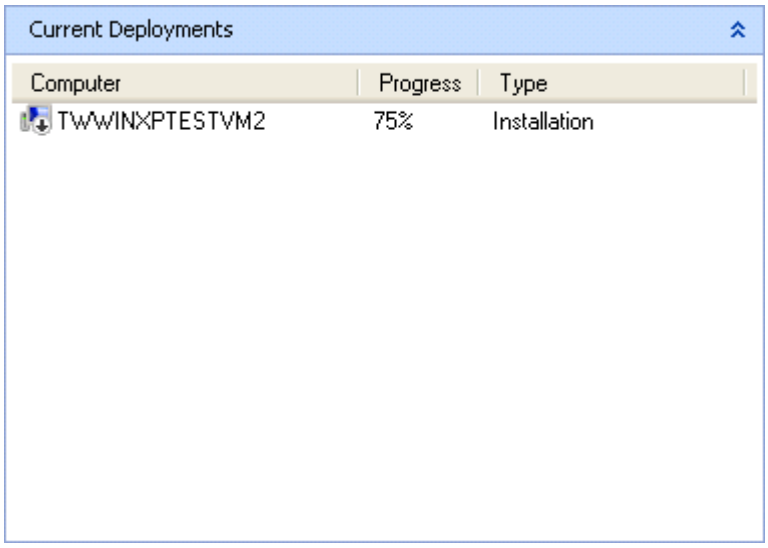
- Current deployment activity
- Queued deployments
- Scheduled deployments
- Deployment history.


GFI EndPointSecurity 4.3
File Configure Help
Discuss this version
Status Activity Configuration Tools Reporting General
General Agents Deployment Statistics
Deployment Status
Monitor the progress of current protection agent deployments. You can also check which deployments are scheduled and go through the deployment history log.
Current Deployments
Computer Progress Type
XP04 75% Installation
Queued Deployments
Computer Type
There are no items to show in this view.
Scheduled Deployments
Computer Deploy on Type
There are no items to show in this view.
Deployment History
Date/Time Computer Type Messages
4/8/2010 4:52:33 PM XP04 Installation Installing the protection agent...
4/8/2010 4:52:33 PM XP04 Installation Installing the deployment service...
4/8/2010 4:52:32 PM XP04 Installation Copying the setup files...
4/8/2010 4:52:32 PM XP04 Installation Preparing files...
4/8/2010 4:52:32 PM XP04 Installation Collecting information...
4/8/2010 4:52:32 PM XP04 Installation Checking if the computer is online...
4/8/2010 4:52:23 PM XP04 Un-installation The un-installation was completed.
4/8/2010 4:52:14 PM XP04 Un-installation Un-installing the protection agent...
2 Computer(s)

Screenshot 47 - Deployment sub-tab

To access the **Deployment** sub-tab, from the GFI EndPointSecurity management console click **Status** tab ► **Deployment**.

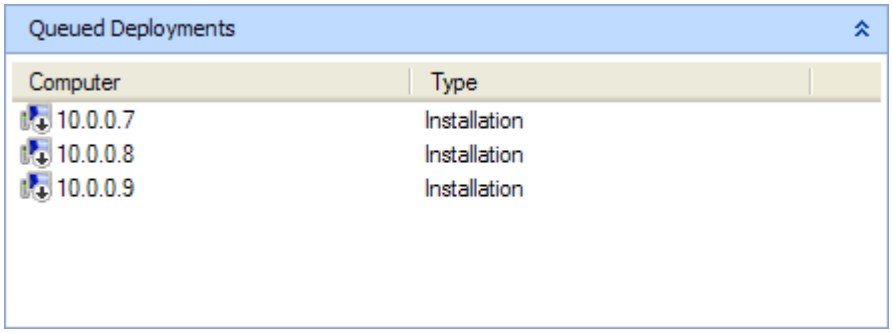
6.4.1 Current Deployments



Screenshot 48 - Current Deployments area

This section displays a list of deployments currently taking place. The information provided includes the computer name, deployment progress and deployment type, i.e., whether the deployment is an installation, un-installation or update.

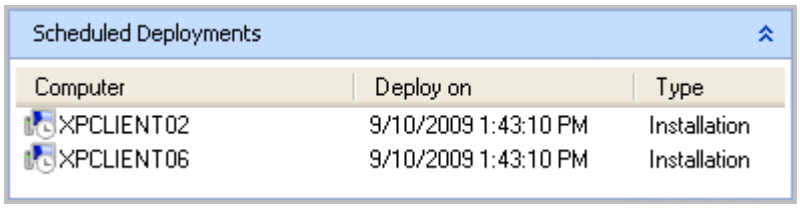
6.4.2 Queued Deployments



Screenshot 49 - Queued Deployments area

This section displays a list of pending deployments. The information provided includes the computer name and deployment type.

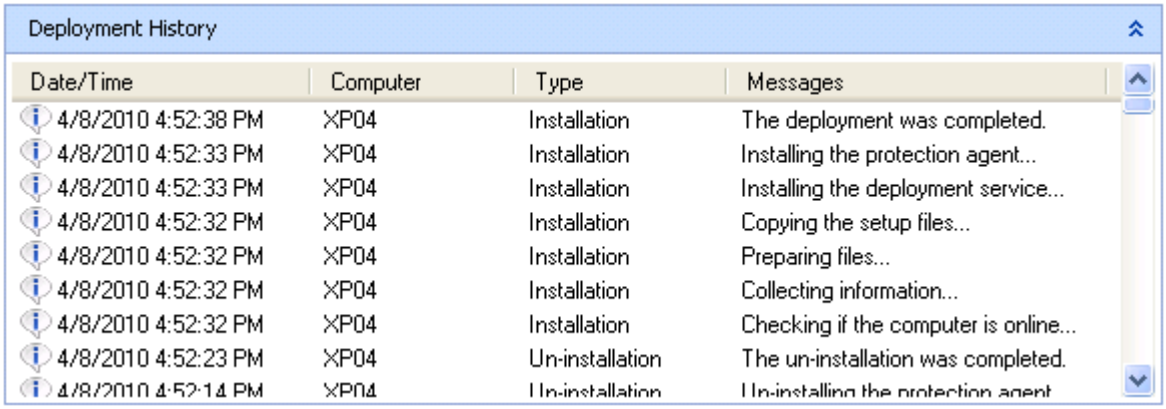
6.4.3 Scheduled Deployments



Screenshot 50 - Scheduled Deployments area

This section displays a list of scheduled deployments. The information provided includes the computer name, scheduled time and deployment type.

6.4.4 Deployment History



Screenshot 51 - Deployment History area

This section displays an audit trail for all stages of all agent or protection policy deployments carried out by GFI EndPointSecurity. The information provided includes the timestamp of each log entry, the computer name, deployment type and errors and information messages generated during the deployment process.

For more information about the error messages that can be encountered upon deployment of agents or protection policies, refer to the **Appendix 1 - Deployment error messages** chapter in this manual.

To remove displayed log entries, right-click in the **Deployment History** area and select **Clear all messages**.

6.5 Statistics

For information about the **Statistics** sub-tab, refer to the **Statistics** section in the **Monitoring device usage activity** chapter.

7 Reporting

The GFI EndPointSecurity ReportPack is a full-fledged reporting add-on to GFI EndPointSecurity. This reporting package can be scheduled to automatically generate graphical IT-level and management reports based on data collected by GFI EndPointSecurity, giving you the ability to report on devices connected to the network, device usage trends by machine or by user, files copied to and from devices (including actual names of files copied) and much more.

To be able to generate reports, you need to download and install the GFI EndPointSecurity ReportPack add-on.

For more information about GFI EndPointSecurity ReportPack and GFI ReportCenter either:

1. From the GFI EndPointSecurity management console, click on the **Reporting** tab

2. In the left pane, select either **GFI EndPointSecurity ReportPack** or **GFI ReportCenter.**

Or visit:

- GFI EndPointSecurity ReportPack:

  http://www.gfi.com/endpointsecurity/esecreportpack.htm

- GFI ReportCenter:

  http://www.gfi.com/page/4713/gfirc

8 Discovering devices

8.1 Introduction

GFI EndPointSecurity provides you with the facility to transparently and rapidly query organizational network endpoints, locating and reporting all devices that are or have been connected to the scanned target computers. The application granularly identifies endpoint devices connected to the target computers, both currently and historically, and displays the detailed information on screen once the scan is complete.

NOTE 1: A discovered target computer can be any computer on the network, and may not be included in any GFI EndPointSecurity protection policy.

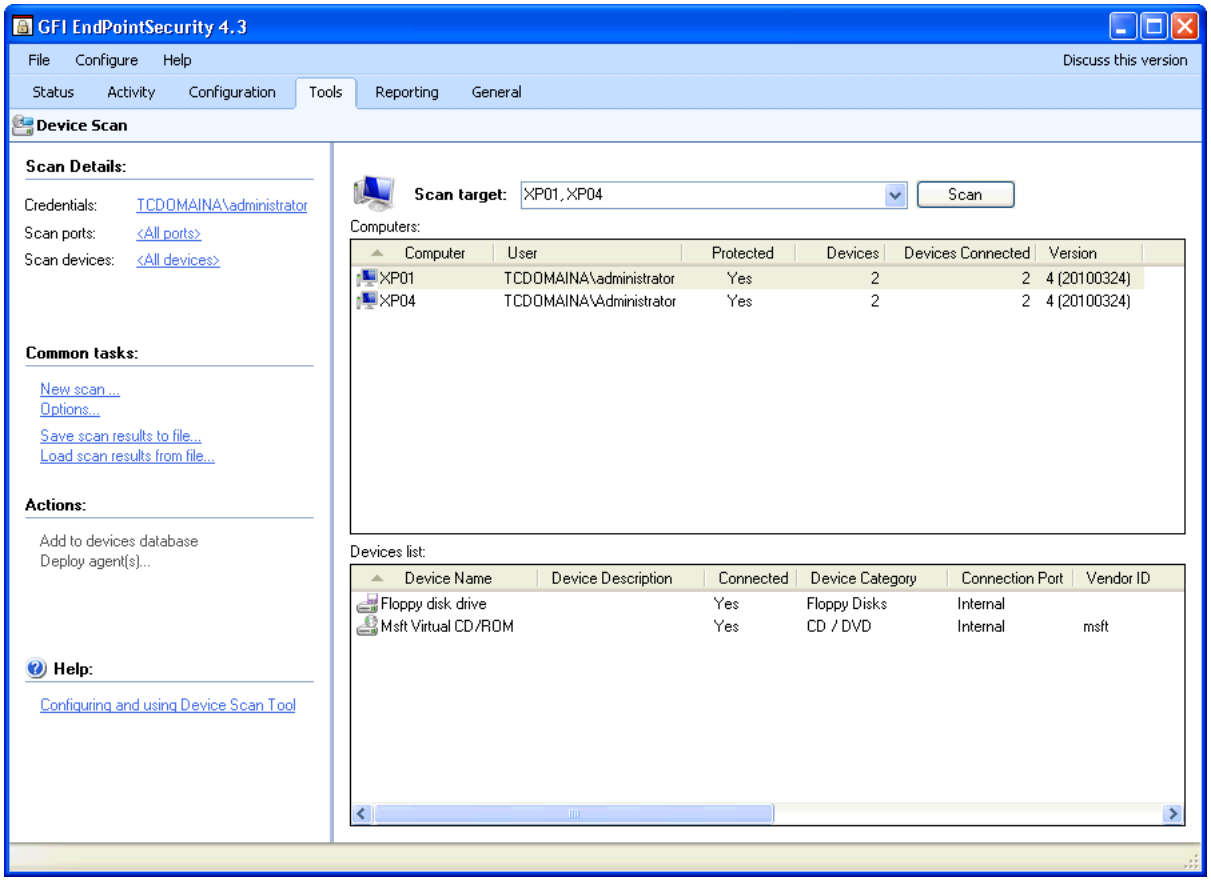
NOTE 2: The device scan must be executed under an account that has administrative privileges over the target computer(s) to be scanned.

8.2 Device Scan

Use the **Device Scan** sub-tab to scan target computers and discover connected devices.

By default:

» GFI EndPointSecurity scans all supported device categories and connectivity ports.

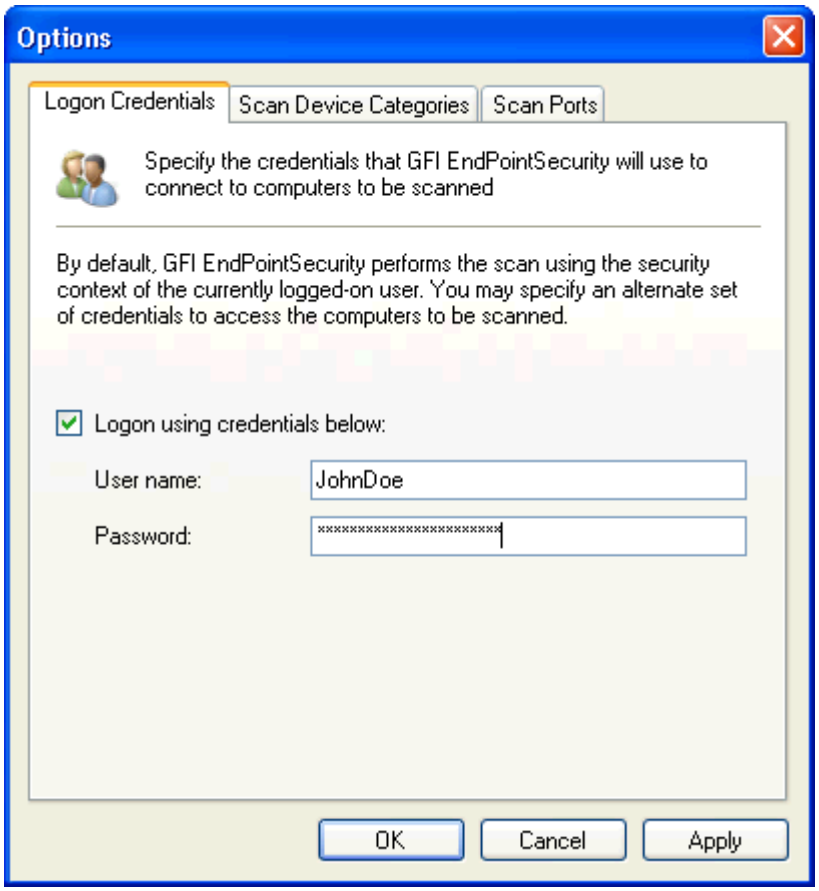


Screenshot 52 - Device Scan sub-tab

8.2.1 Running a Device Scan

To carry out a device scan:

1. From the GFI EndPointSecurity management console, click on the **Tools** tab.
2. Click on the **Device Scan** sub-tab.
3. In the left pane, click on the **Credentials** hyperlink in the **Scan Details** section.

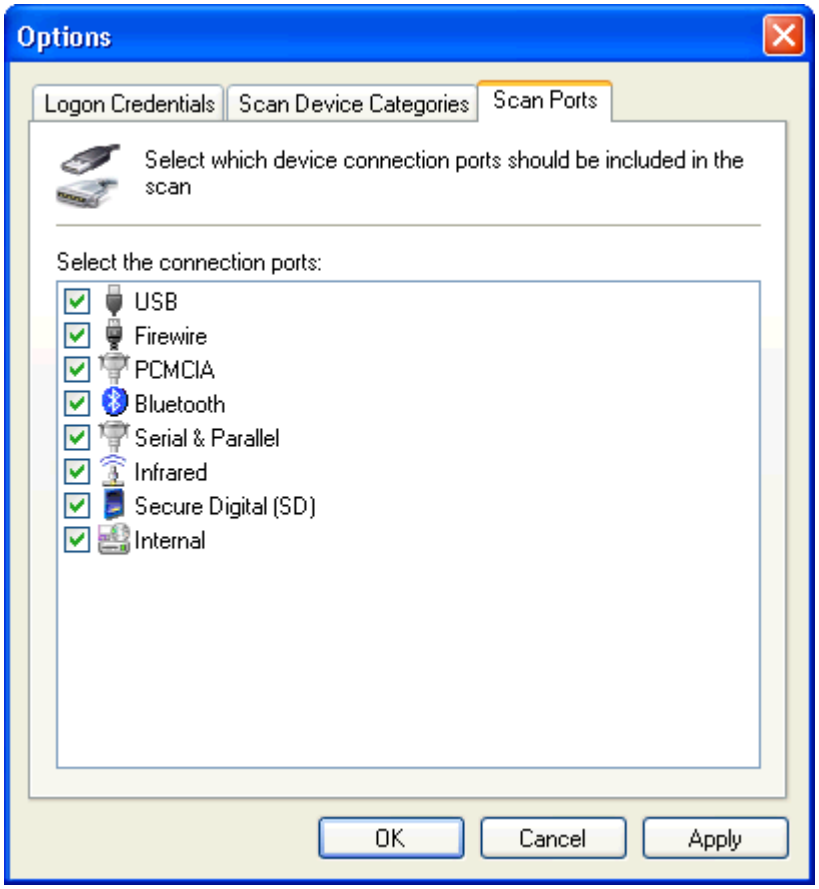

Options
Logon Credentials
Scan Device Categories
Scan Ports
Specify the credentials that GFI EndPointSecurity will use to connect to computers to be scanned
By default, GFI EndPointSecurity performs the scan using the security context of the currently logged-on user. You may specify an alternate set of credentials to access the computers to be scanned.
Logon using credentials below:
User name:
JohnDoe
Password:
OK
Cancel
Apply

Screenshot 53 - Options - Logon Credentials tab

4. In the **Options** dialog enable the **Logon using credentials below** and key in the credentials that GFI EndPointSecurity will use to connect to the target computers to be scanned, and click **OK**.

By default, GFI EndPointSecurity performs the scan using the logon credentials of the currently logged-on user account from which GFI EndPointSecurity application is running.

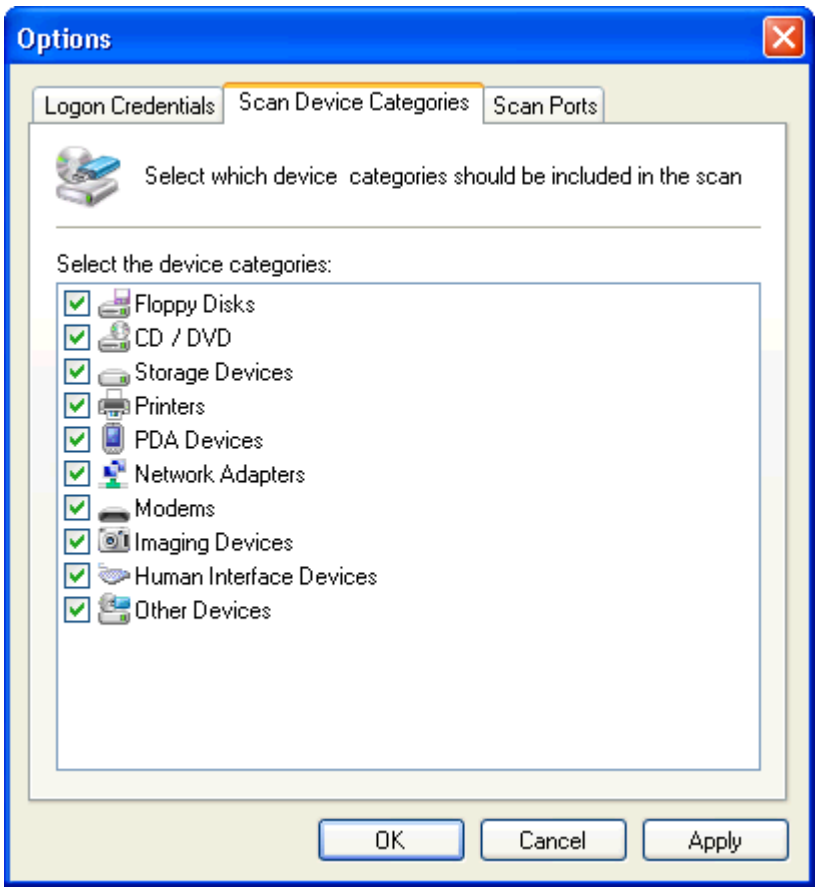
5. In the left pane, click on the **Scan ports** hyperlink in the **Scan Details** section.



Screenshot 54 - Options - Scan Ports tab

6. In the **Options** dialog enable or disable the required device connection ports (that might be used by devices to connect to the target computers) to be scanned, and click **OK**.

7. In the left pane, click on the **Scan devices** hyperlink in the **Scan Details** section.



Screenshot 55 - Options - Scan Device Categories tab

8. In the **Options** dialog enable or disable the required device categories (of the devices that might be connected to the target computers) to be scanned, and click **OK**.

9. To specify scan target computers:

- Option 1: In the right pane, key in the computer name or IP address of the target computer(s) in the **Scan target** text box, and click the **Scan** button to start the device discovery process.
- Option 2: In the left pane, click the **New scan…** hyperlink and continue to specify the desired scan target(s). The available options are a single, a range or a list of computers.

8.2.2 Device Scan results

Device Scan results are displayed in two sections:

- Computers
- Devices list

Computers:

Computer	User	Protected	Devices	Devices Connected	Version
XP01	TCDOMAINA\administrator	Yes	2	2	4 (20100324)
XP04	TCDOMAINA\Administrator	Yes	2	2	4 (20100324)

Screenshot 56 - Computers area

Computers

This section displays device scan summary results for every scanned target computer, including:

- The computer name / IP address
- The user currently logged on
- Protection status, i.e., whether the computer is included in a GFI EndPointSecurity protection policy
- Total number of devices currently and historically connected
- Number of devices currently connected.

If a scanned target computer is not included in any GFI EndPointSecurity protection policy, you can choose to deploy a protection policy to the computer. To do this:

1. Right-click on the relevant computer name / IP address under the **Computer** column.

2. Select **Deploy agent(s)…**

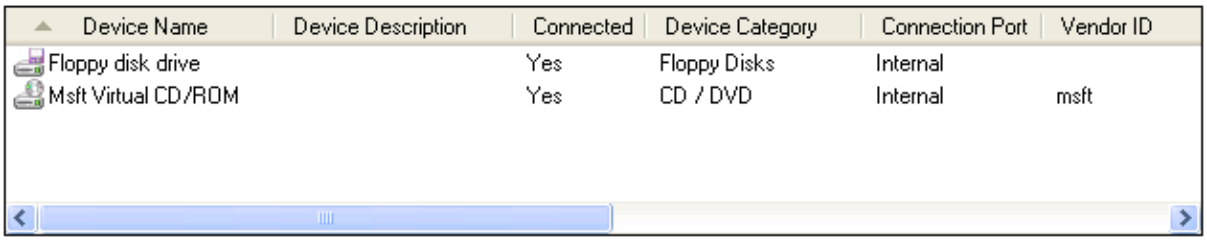
3. Select the protection policy to deploy. Click **Next** to continue and **Finish** to start deployment.

Devices list

This section displays a detailed list of discovered devices for every scanned computer, including:

- Device name, description and category
- Connectivity port
- Connection status, i.e., whether the device is currently connected or not.

Devices list:

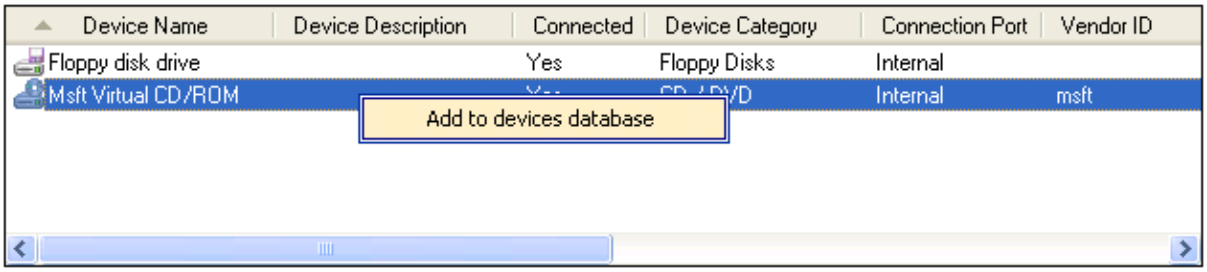


Screenshot 57 - Devices list area

8.2.3 Adding discovered devices in devices database

You can select one or more of the discovered devices from the **Devices list** and add them to the devices database. These devices are then retrieved from this database when GFI EndPointSecurity lists the devices currently connected to the target computers for the blacklist and whitelist features. For information on the blacklist and whitelist features, refer to the **Configuring device blacklist** or **Configuring device whitelist** section respectively in the **Customizing protection policies** chapter.

Devices list:



Screenshot 58 - Devices list area - Add device to devices database

To add devices to the devices database:

1. Select one or more devices to add to the devices database from the **Devices list** section.
2. Right-click on the selected devices and select **Add to devices database**, and click **OK**.

9 Customizing protection policies

9.1 Introduction

All protection policies created within GFI EndPointSecurity are fully customizable and can be configured to suit your company's device access security policies. This also applies for the default policy that is used by the auto discovery feature of GFI EndPointSecurity. In this chapter you will learn how to:

- Configure controlled device categories
- Configure controlled connectivity ports
- Configure power users
- Configure access permissions for device categories
- Configure access permissions for connectivity ports
- Configure access permissions for specific devices
- View access permissions
- Configure priorities for permissions
- Configure device blacklist
- Configure device whitelist
- Configure temporary access privileges
- Configure file-type filters
- Configure security encryption
- Configure event logging
- Configure alerts
- Set a policy as the default policy.

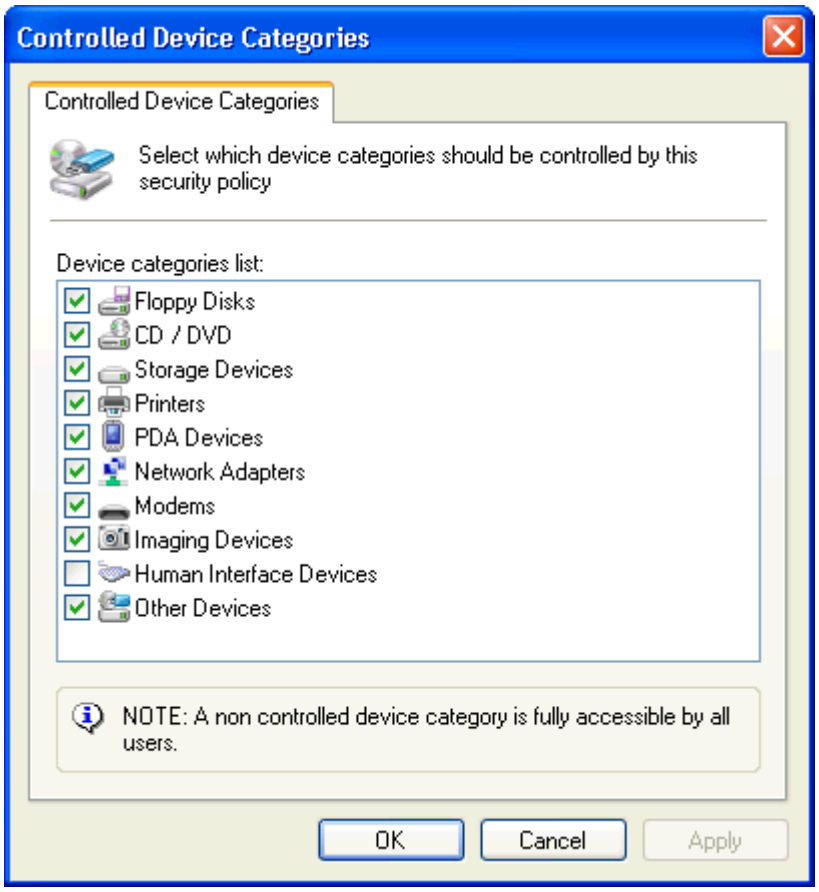
9.2 Configuring controlled device categories

GFI EndPointSecurity provides you with the facility to specify which supported device categories should be controlled or not by a protection policy. You can do this on a policy by policy basis.

Unspecified devices will be fully accessible from the target computers covered by the protection policy. As a result, GFI EndPointSecurity cannot monitor and block devices falling in a category that is not controlled by the protection policy.

To configure which devices will be controlled by a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Protection Policies** sub-tab.
3. From the left pane, select the protection policy to configure.
4. Click on the **Security** sub-node.
5. From the left pane, click the **Edit controlled device categories…** hyperlink in the **Common tasks** section.



Screenshot 59 - Controlled Device Categories options

6. In the **Controlled Device Categories** dialog, enable or disable the required device categories that will be controlled by the protection policy, and click **OK**.

If **Human Interface Devices** is enabled and access is denied, users will not be able to use USB keyboards and mice connected to target computers protected by this policy.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Computers** sub-tab.
3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

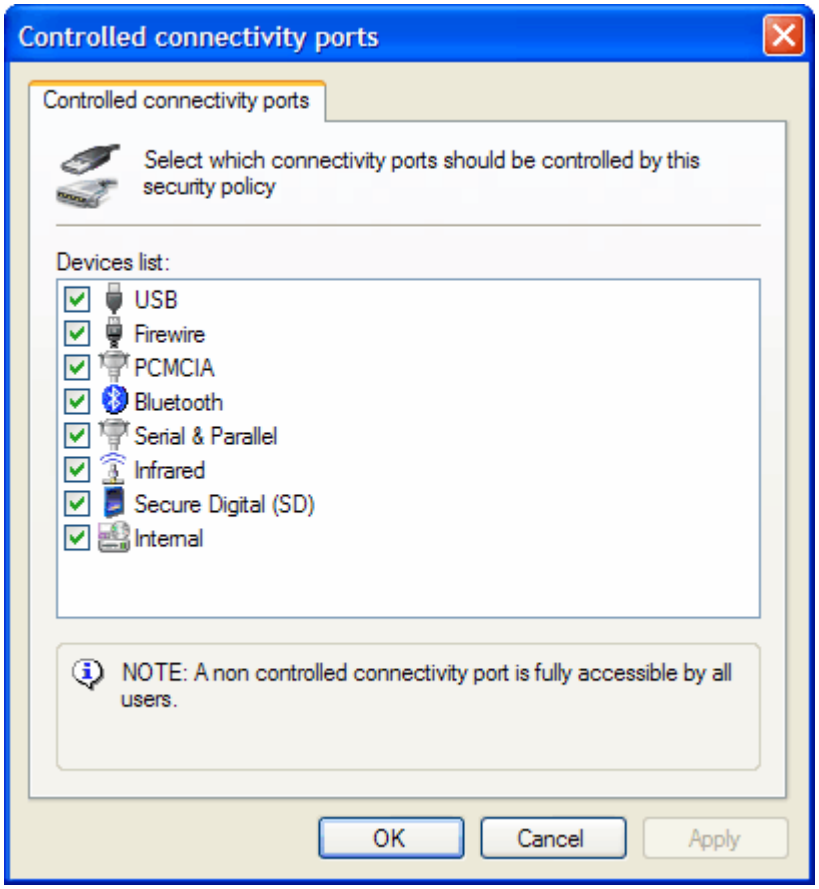
9.3 Configuring controlled connectivity ports

GFI EndPointSecurity provides you with the facility to specify which supported connectivity ports should be controlled or not by a protection policy. You can do this on a policy by policy basis.

Unspecified ports will be fully accessible from the target computers covered by the protection policy. As a result, GFI EndPointSecurity cannot monitor and block devices connected to a port that is not controlled by the protection policy.

To configure which ports will be controlled by a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Protection Policies** sub-tab.
3. From the left pane, select the protection policy to configure.
4. Click on the **Security** sub-node.
5. From the left pane, click the **Edit controlled ports…** hyperlink in the **Common tasks** section.



Screenshot 60 - Controlled connectivity ports options

6. In the **Controlled connectivity ports** dialog, enable or disable the required connectivity ports that will be controlled by the protection policy, and click **OK**.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.4 Configuring power users

GFI EndPointSecurity provides you with the facility to specify Active Directory (AD) users and/or user groups, or local users and/or groups schema as power users. Power users are automatically given full access to devices connected to any target computer covered by the protection policy. You can define sets of power users on a policy by policy basis.

You should exercise caution when using this feature, since incorrectly specifying a user as a power user will lead to that user overriding all restrictions of the relevant protection policy.

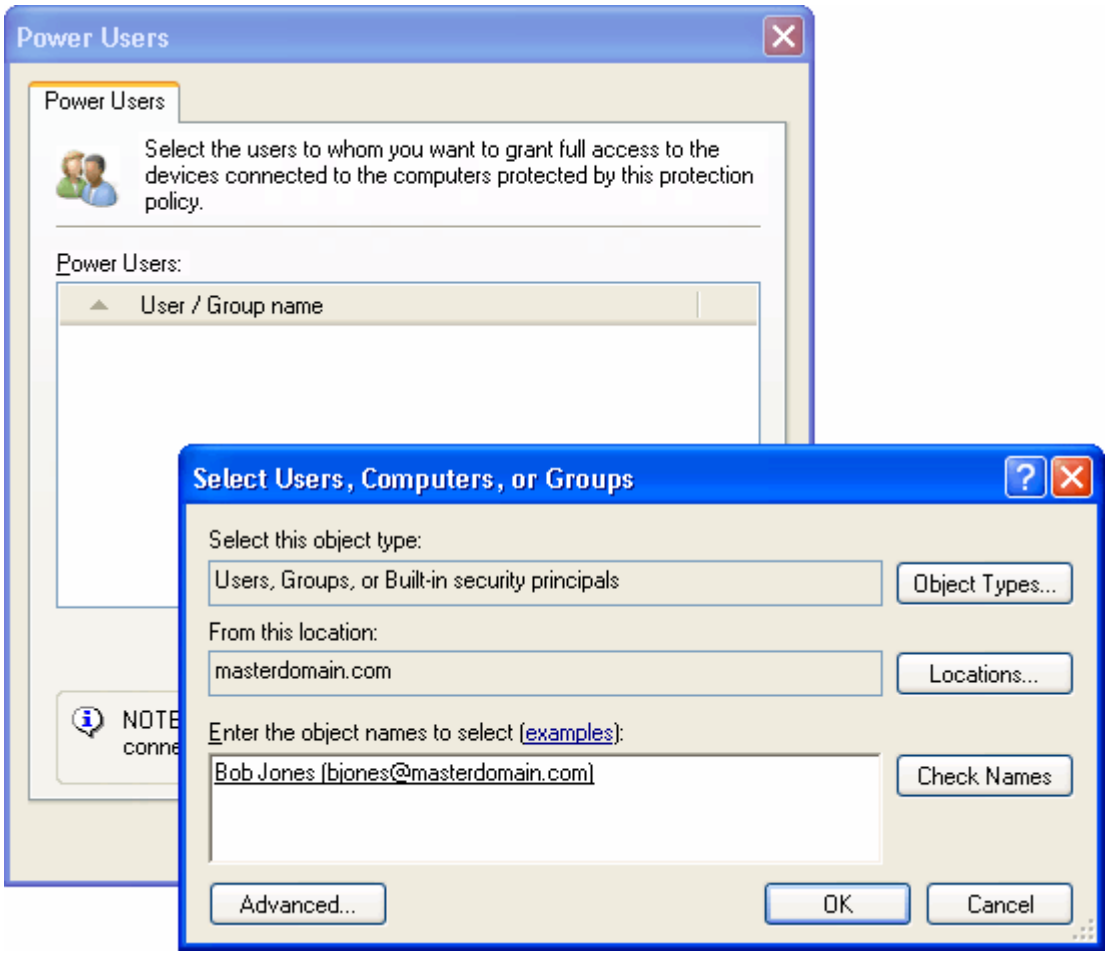
To specify power users within a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy for which you want to specify power users.

4. From the right pane, click the **Power users** hyperlink in the **Security** section.



Screenshot 61 - Power users options

5. In the **Power Users** dialog:

   - » Option 1: Click **Add…** to specify the user(s)/group(s) that will be set as power users for this protection policy, and click **OK**.
   - » Option 2: Highlight user(s)/group(s) and click **Remove** to demote from power users, and click **OK**.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Computers** sub-tab.
3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.5 Configuring access permissions for device categories

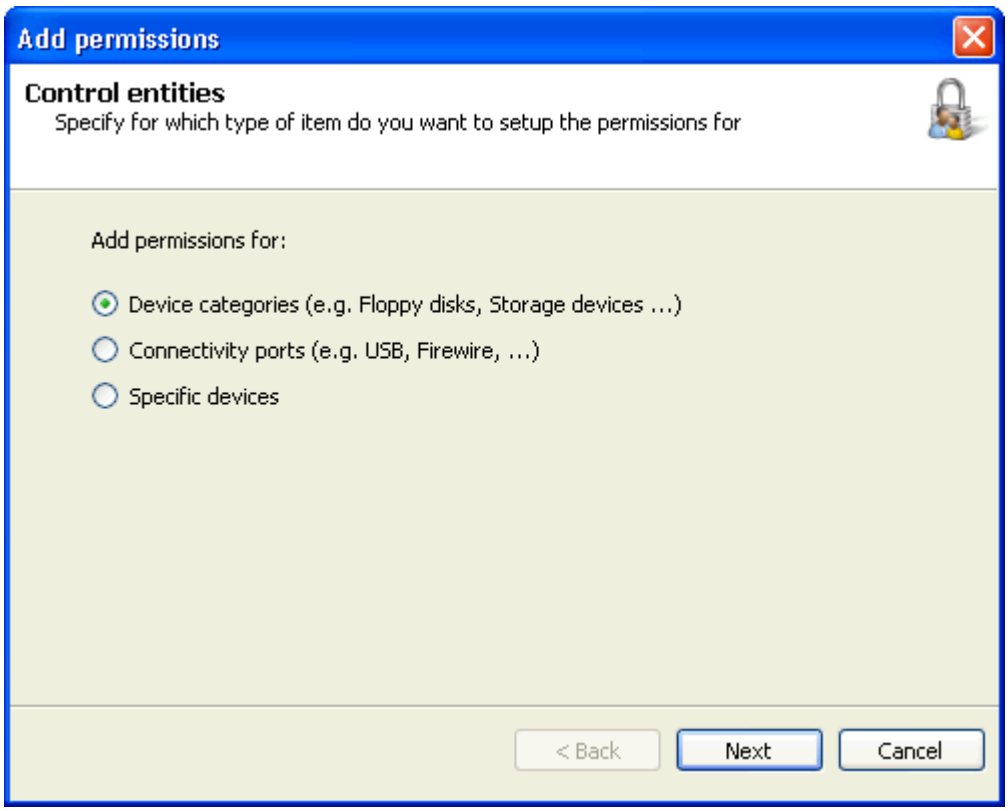
GFI EndPointSecurity provides you with the facility to set permissions by device categories to Active Directory (AD) users and/or user groups, or local users and/or groups schema. You can do this on a policy by policy basis.

When a device category is not set to be controlled by the particular security policy, the relevant entry is disabled. For more information on how to add or remove control over device categories, refer to the Configuring controlled device categories section in this chapter.

To configure device category access permissions for users within a specific protection policy:

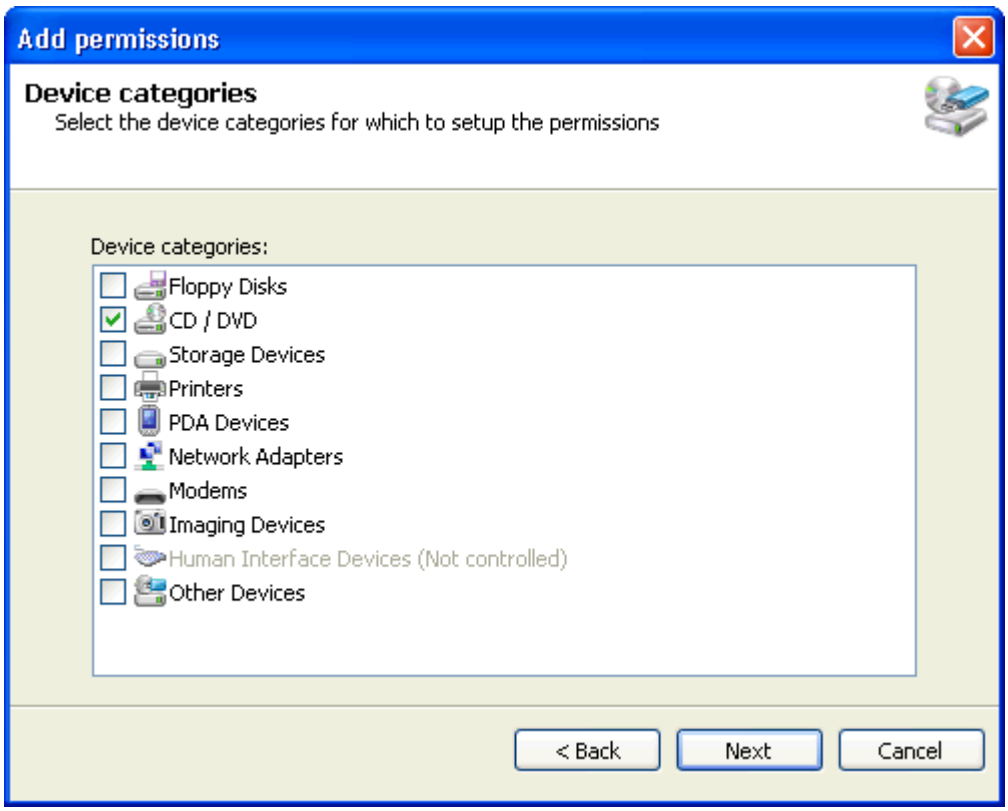
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Protection Policies** sub-tab.
3. From the left pane, select the protection policy to configure.
4. Click on the **Security** sub-node.

5. From the left pane, click the **Add permission(s)…** hyperlink in the **Common tasks** section.


Add permissions
Control entities
Specify for which type of item do you want to setup the permissions for
Add permissions for:
Device categories (e.g. Floppy disks, Storage devices ...)
Connectivity ports (e.g. USB, Firewire, ...)
Specific devices
< Back
Next
Cancel

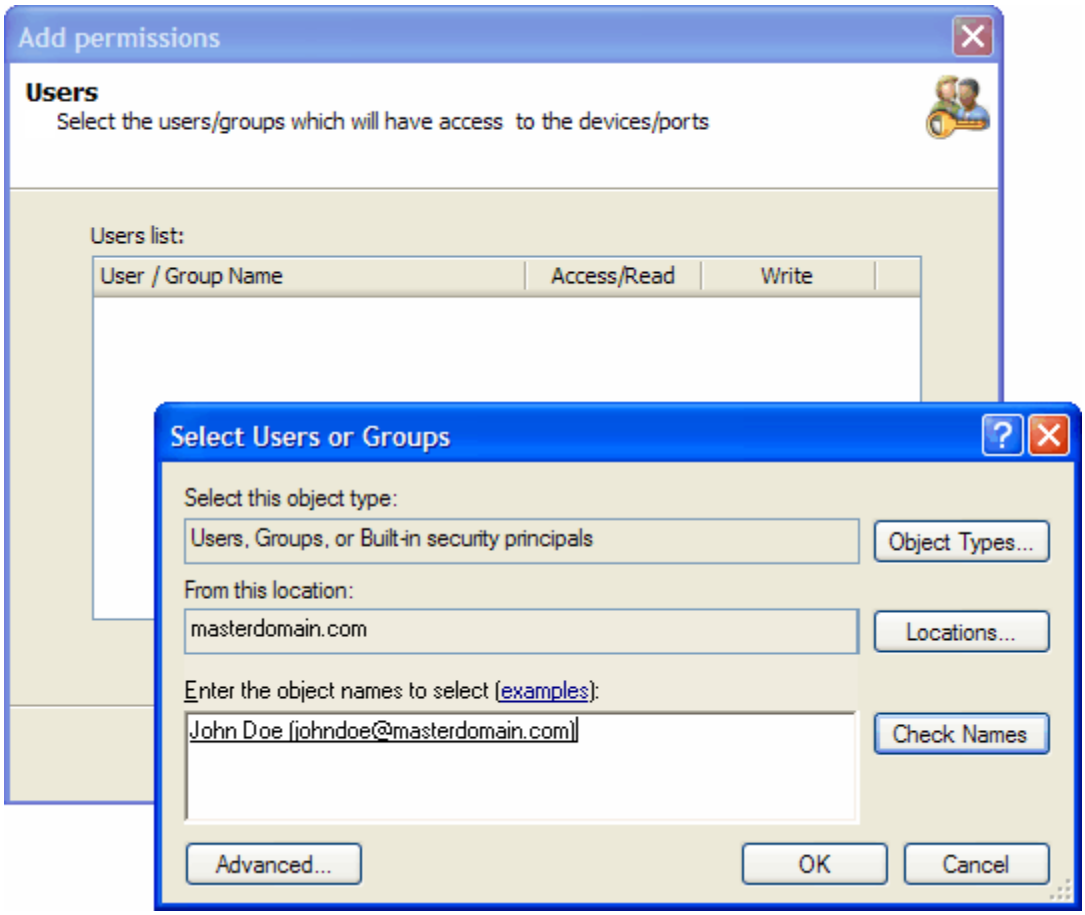
Screenshot 62 - Add permissions options - Control entities

6. In the **Add permissions** dialog select the **Device categories** option and click **Next** to continue.



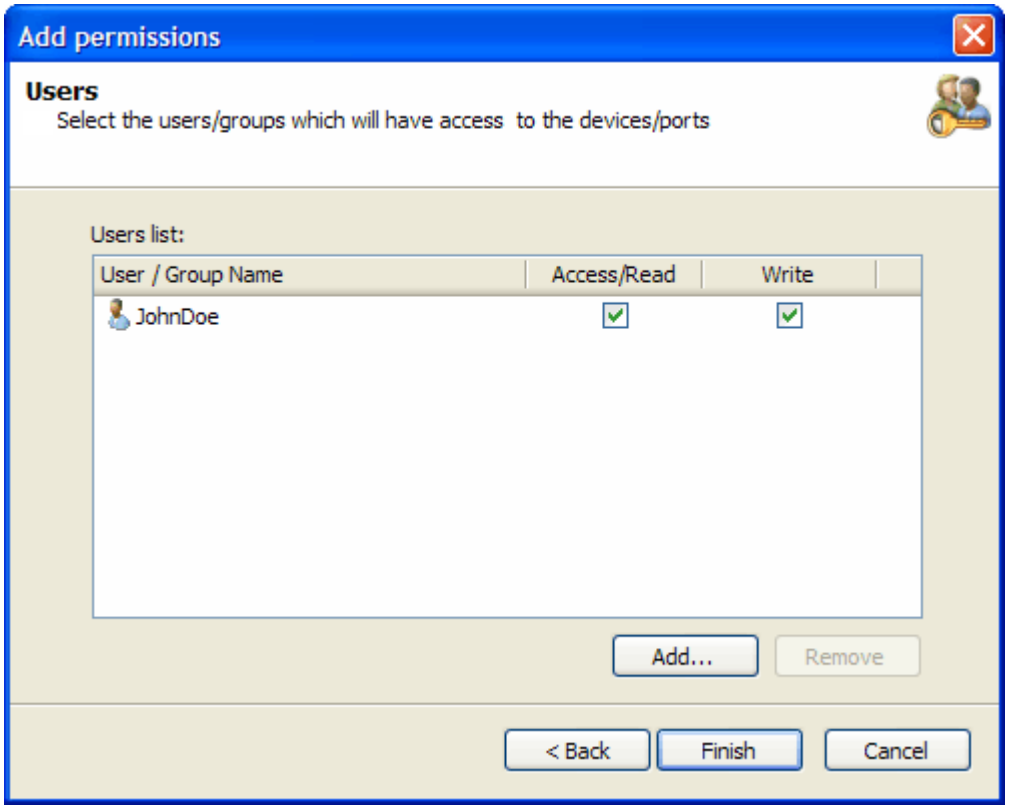
Screenshot 63 - Add permissions options - Device categories

7. Enable or disable the required device categories for which to configure permissions, and click **Next**.



Screenshot 64 - Add permissions options - Users

8. Click **Add...** to specify the user(s)/group(s) that will have access to the device categories specified in this protection policy, and click **OK**.



Screenshot 65 - Add permissions options - Users

9. Enable or disable the **Access/Read** and **Write** permissions for each user/group you specified and click **Finish**.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.6 Configuring access permissions for connectivity ports

GFI EndPointSecurity provides you with the facility to set permissions by connectivity ports to Active Directory (AD) users and/or user groups, or local users and/or groups schema. You can do this on a policy by policy basis.

When a connectivity port is not set to be controlled by the particular security policy, the relevant permission is disabled. For more information on how to add or remove control over connectivity ports, refer to the **Configuring controlled connectivity ports** section in this chapter.

To configure connectivity port usage permissions for users within a specific protection policy:

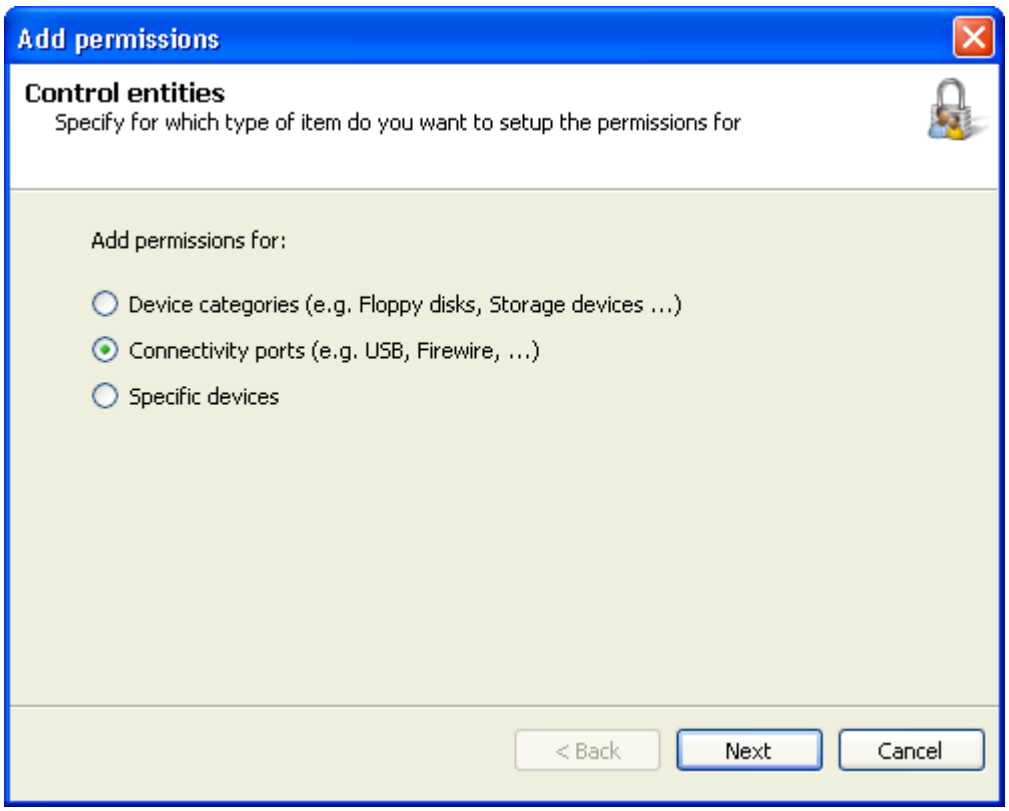
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy to configure.

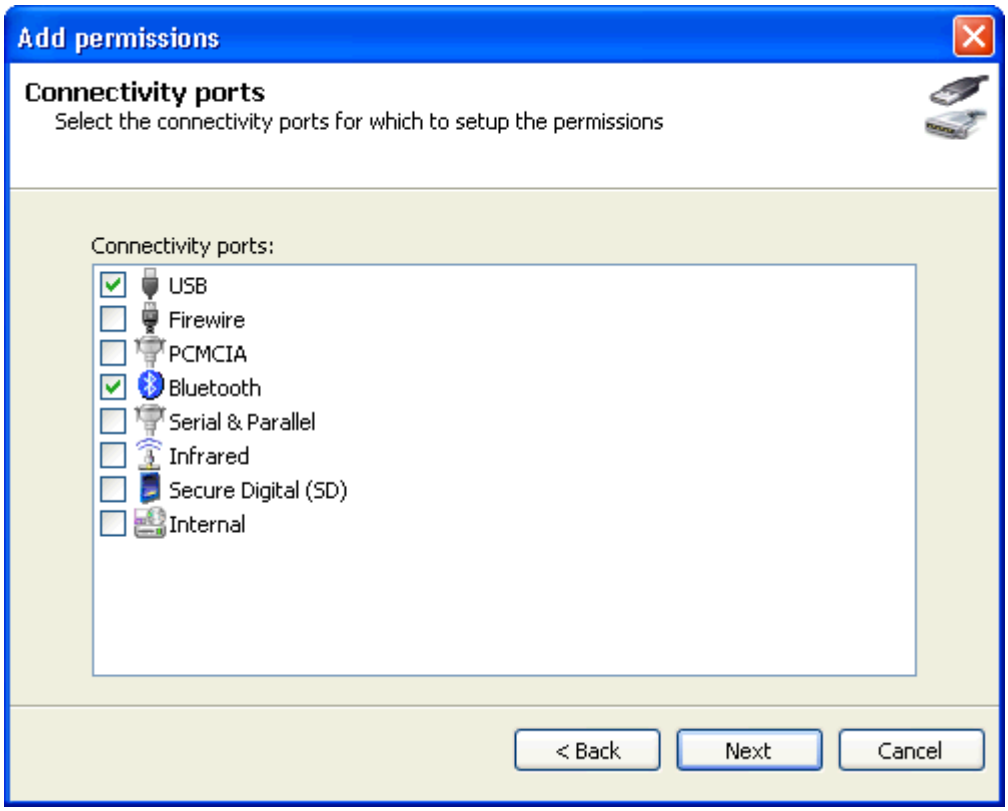
4. Click on the **Security** sub-node.

5. From the left pane, click the **Add permission(s)…** hyperlink in the **Common tasks** section.


Add permissions
Control entities
Specify for which type of item do you want to setup the permissions for
Add permissions for:
Device categories (e.g. Floppy disks, Storage devices ...)
Connectivity ports (e.g. USB, Firewire, ...)
Specific devices
< Back
Next
Cancel

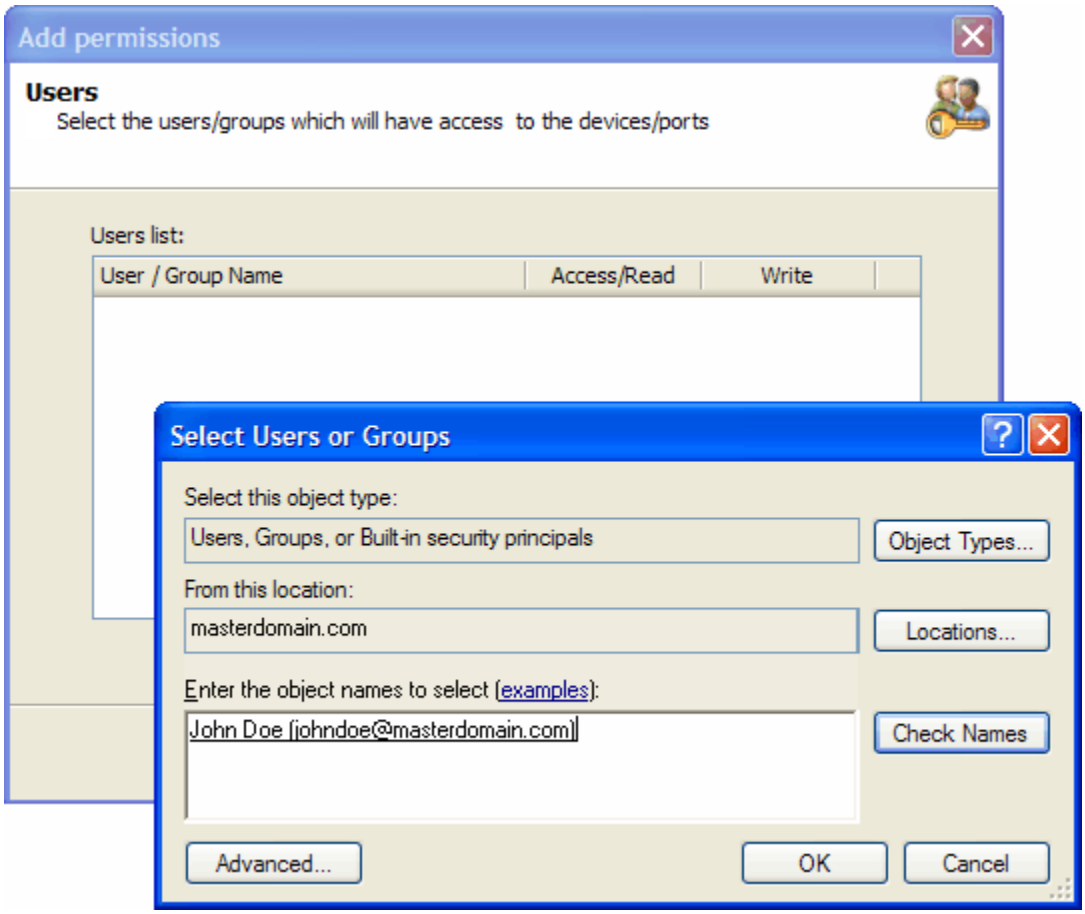
Screenshot 66 - Add permissions options - Control entities

6. In the **Add permissions** dialog select the **Connectivity ports** option and click **Next** to continue.



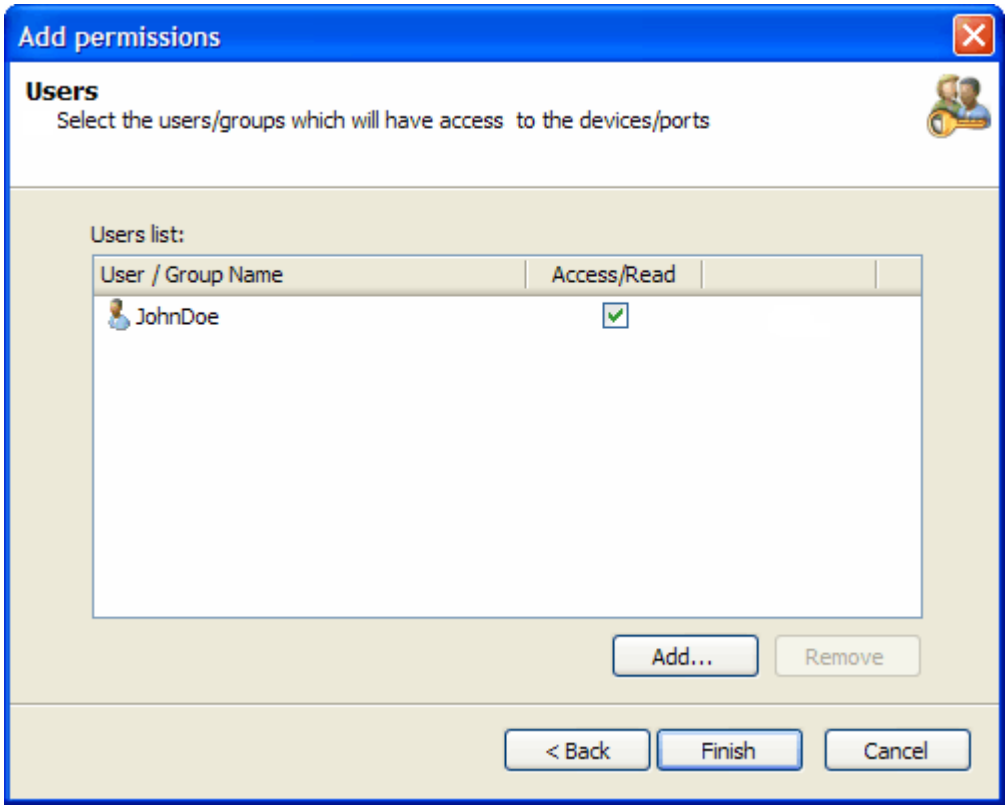
Screenshot 67 - Add permissions options - Connectivity ports

7. Enable or disable the required connectivity ports for which to configure permissions, and click **Next**.



Screenshot 68 - Add permissions options - Users

8. Click **Add...** to specify the user(s)/group(s) that will have access to the connectivity ports specified in this protection policy, and click **OK**.



Screenshot 69 - Add permissions options - Users

9. Enable or disable the **Access/Read** permissions for each user/group you specified, and click **Finish**.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers**… hyperlink in the **Common tasks** section.

9.7 Configuring access permissions for specific devices

GFI EndPointSecurity provides you with the facility to set permissions by specific devices to Active Directory (AD) users and/or user groups, or local users and/or groups schema. You can do this on a policy by policy basis.

For example, you can assign read-only permissions to a specific company approved USB pen drive. Attempts to use any other non-approved USB pen drives will be blocked.

For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring access permissions for specific devices. For more information about the device scan feature, refer to the Discovering devices chapter in this manual.

To configure specific device access permissions for users within a specific protection policy:

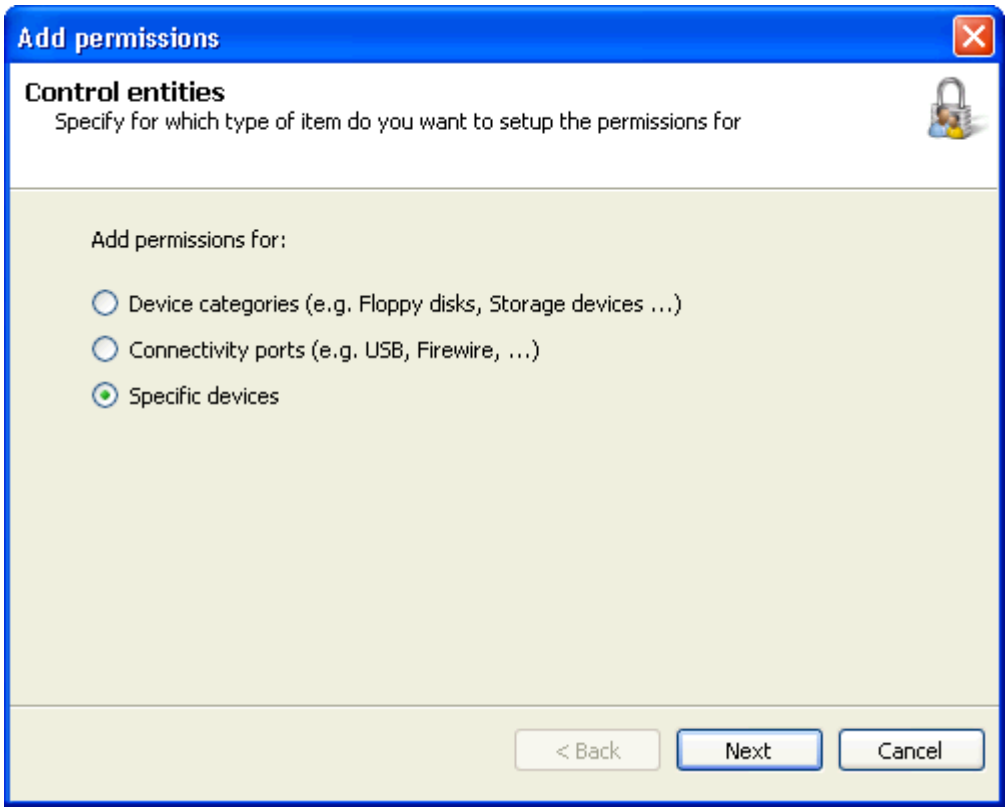
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy to configure.

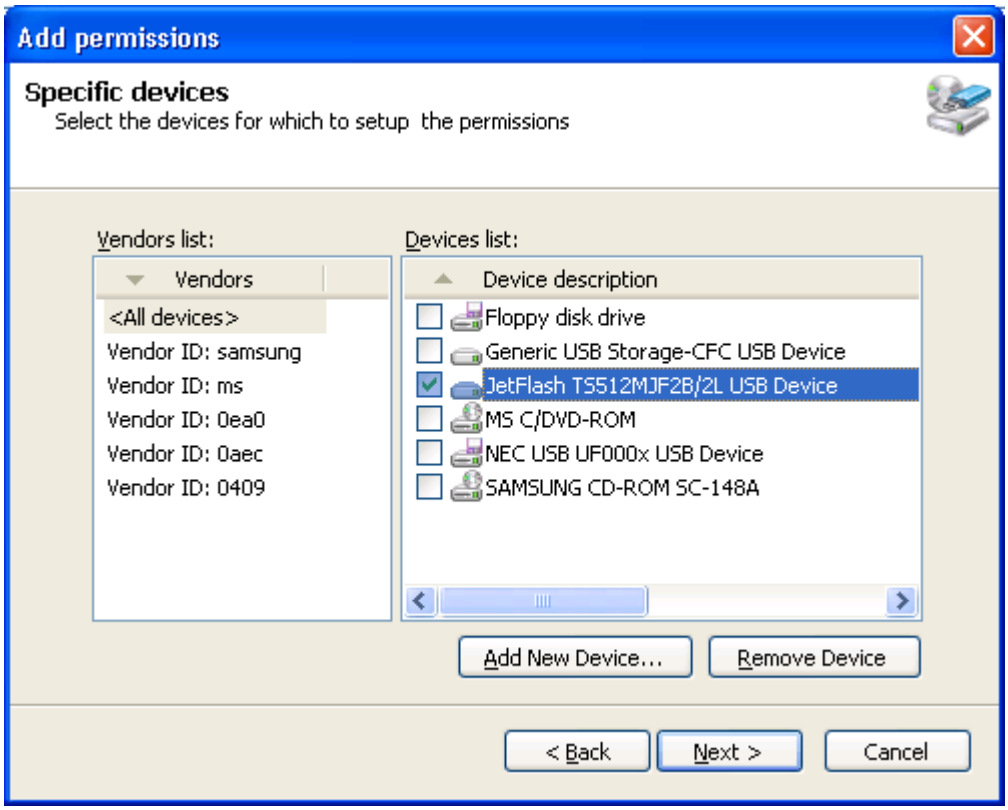
4. Click on the **Security** sub-node.

5. From the left pane, click the **Add permission(s)**… hyperlink in the **Common tasks** section.


Add permissions
Control entities
Specify for which type of item do you want to setup the permissions for
Add permissions for:
Device categories (e.g. Floppy disks, Storage devices ...)
Connectivity ports (e.g. USB, Firewire, ...)
Specific devices
< Back
Next
Cancel

Screenshot 70 - Add permissions options - Control entities

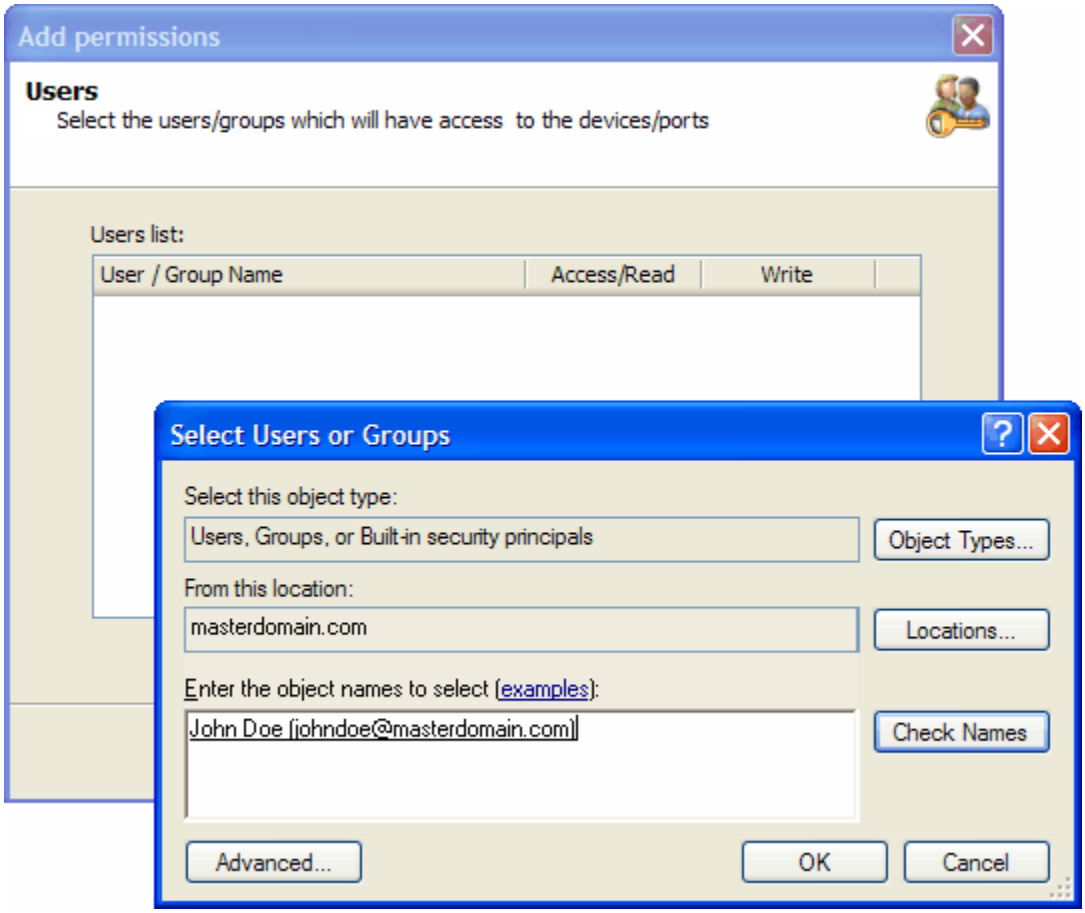
6. In the **Add permissions** dialog select the **Specific devices** option and click **Next** to continue.



Screenshot 71 - Add permissions options - Specific devices

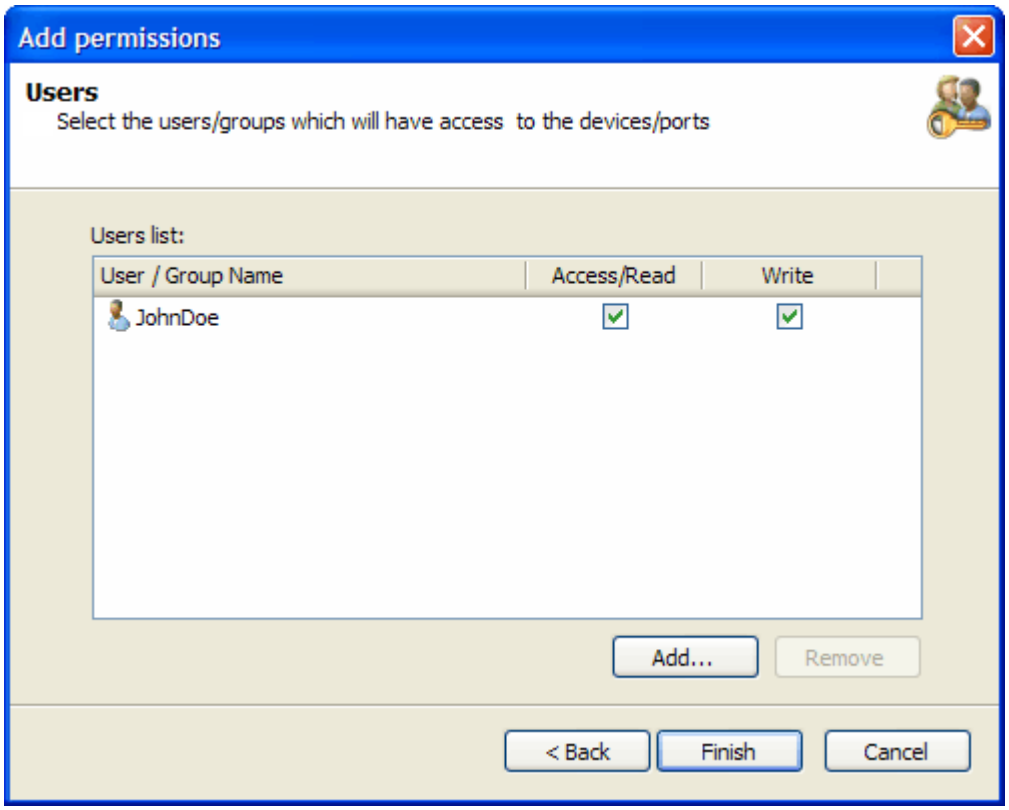
7. Enable or disable the required devices from the **Devices list**, for which to configure permissions, and click **Next**.

If a required device is not listed, click **Add New Device**… to specify the details of the device for which to configure permissions, and click **OK**.



Screenshot 72 - Add permissions options - Users

8. Click **Add…** to specify the user(s)/group(s) that will have access to the specific devices specified in this protection policy, and click **OK**.



Screenshot 73 - Add permissions options - Users

9. Enable or disable the **Access/Read** and **Write** permissions for each user/group you specified and click **Finish**.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.8 Viewing access permissions

GFI EndPointSecurity provides you with the facility to view all permissions assigned to Active Directory (AD) users and/or user groups, or local users and/or groups schema. You can do this on a policy by policy basis.

When a device category or connectivity port is not set to be controlled by the particular security policy, the relevant permission is disabled. For more information on how to add or remove control over device categories or connectivity ports, refer to the Configuring controlled device categories section or the Configuring controlled connectivity ports section in this chapter.

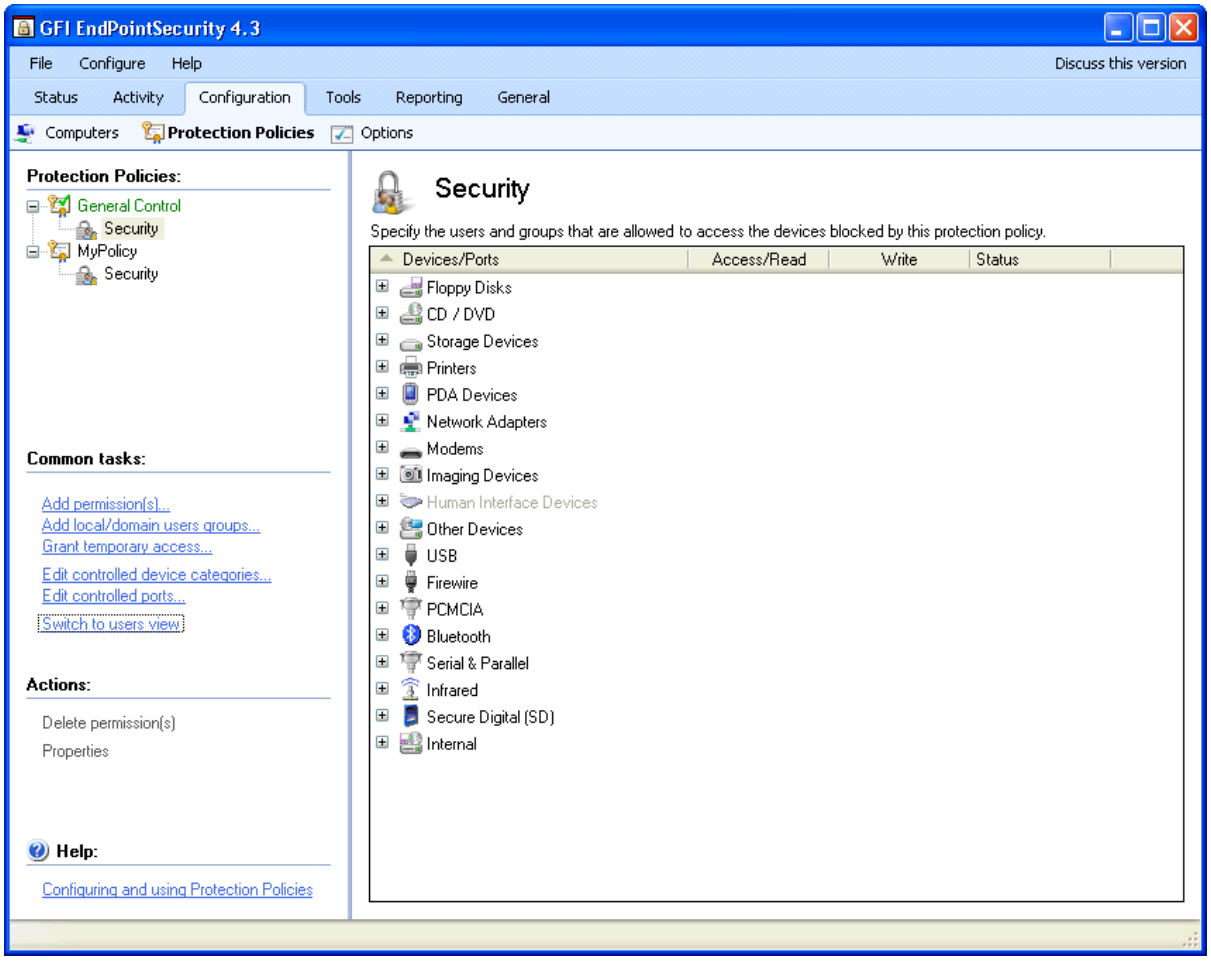
To view all permissions assigned to users within a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

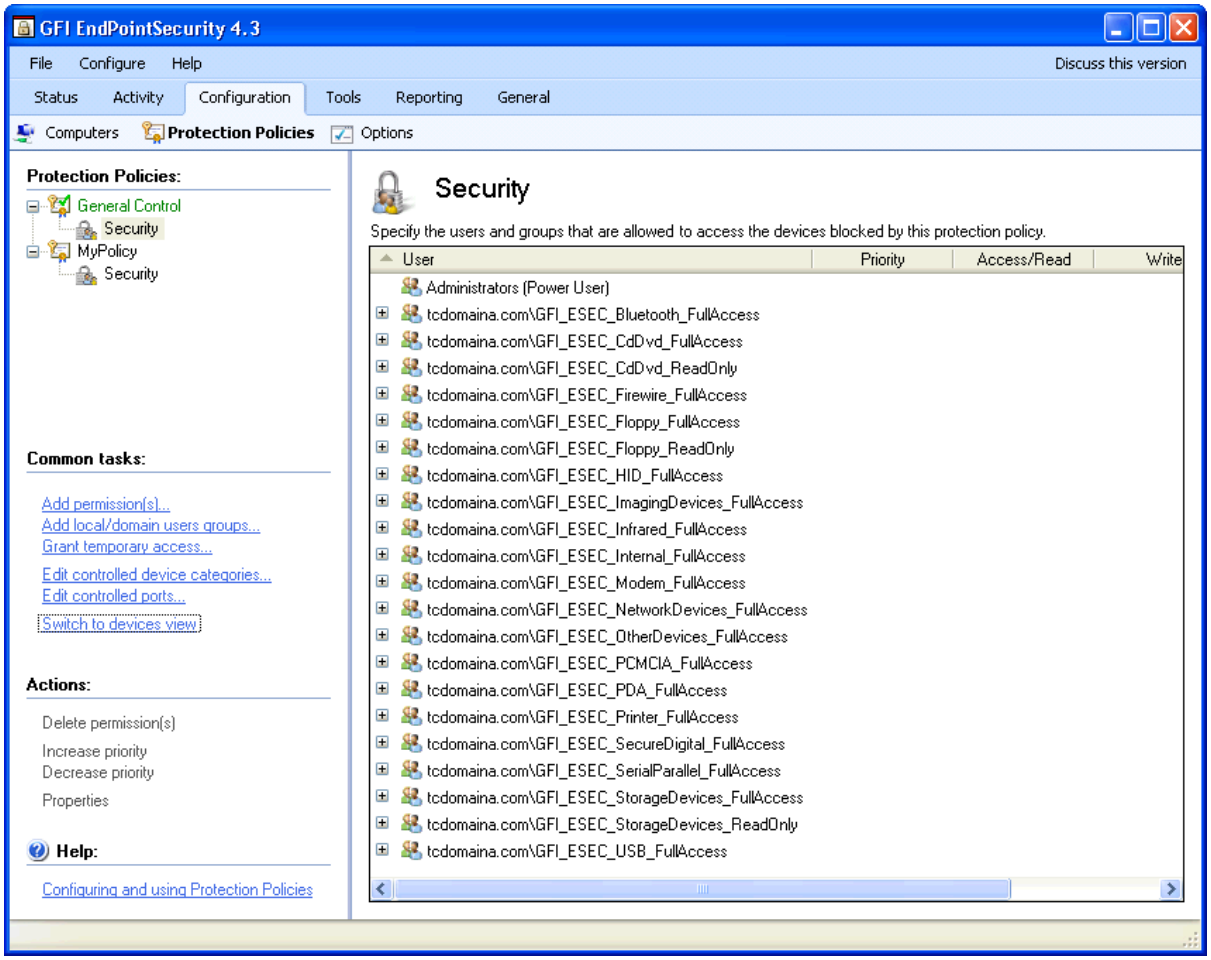
2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy for which you want to view the permissions set.

4. Click on the **Security** sub-node. In the right pane you can view all the set permissions for this protection policy.



Screenshot 74 - Protection Policies sub-tab - devices view



Screenshot 75 - Protection Policies sub-tab - users view

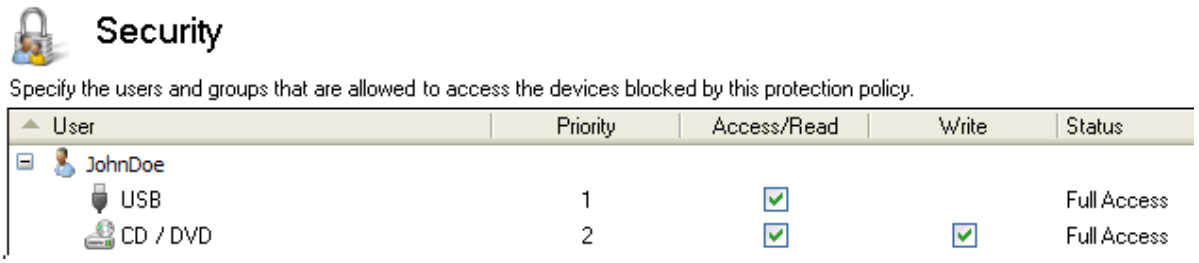
5. From the left pane, click the **Switch to devices view** hyperlink or the **Switch to users view** hyperlink in the **Common tasks** section, to switch grouping of permissions by devices/ports or users.

In users view, you will also see any power users specified within the policy.

9.9 Configuring priorities for permissions

GFI EndPointSecurity provides you with the facility to prioritize any permissions assigned to Active Directory (AD) users and/or user groups, or local users and/or groups schema. You can do this on a policy by policy basis and on a user by user basis.

For example, for a specific user specified within a specific protection policy, you may decide to give priority 1 to USB port permissions, and priority 2 to CD/DVD drive permissions. This means that if the user connects an external CD/DVD drive via the USB port to the target computer, permissions for the USB port will take precedence over permissions for the CD/DVD drive.



Screenshot 76 - Protection Policies sub-tab - Security area

To prioritize permissions assigned to users within a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy for which you want to set priorities for the permissions set.

4. Click on the **Security** sub-node.

5. From the left pane, click the **Switch to users view** hyperlink in the **Common tasks** section, to switch grouping of permissions by users.

6. Right-click in the **Security** section and select **Expand all**.

7. Highlight the required device or port.

8. From the left pane, click the **Increase priority** hyperlink or the **Decrease priority** hyperlink in the **Actions** section.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers**… hyperlink in the **Common tasks** section.

9.10 Configuring device blacklist

GFI EndPointSecurity provides you with the facility to specify which device(s) can be made inaccessible to everyone. The blacklist is granular, so you can even blacklist a specific device with a specific serial number. You can do this on a policy by policy basis.

For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring blacklisted devices. For more information about the device scan feature, refer to the Discovering devices chapter in this manual.

Power users will override any blacklisted devices, and thus will be able to access any blacklisted devices.

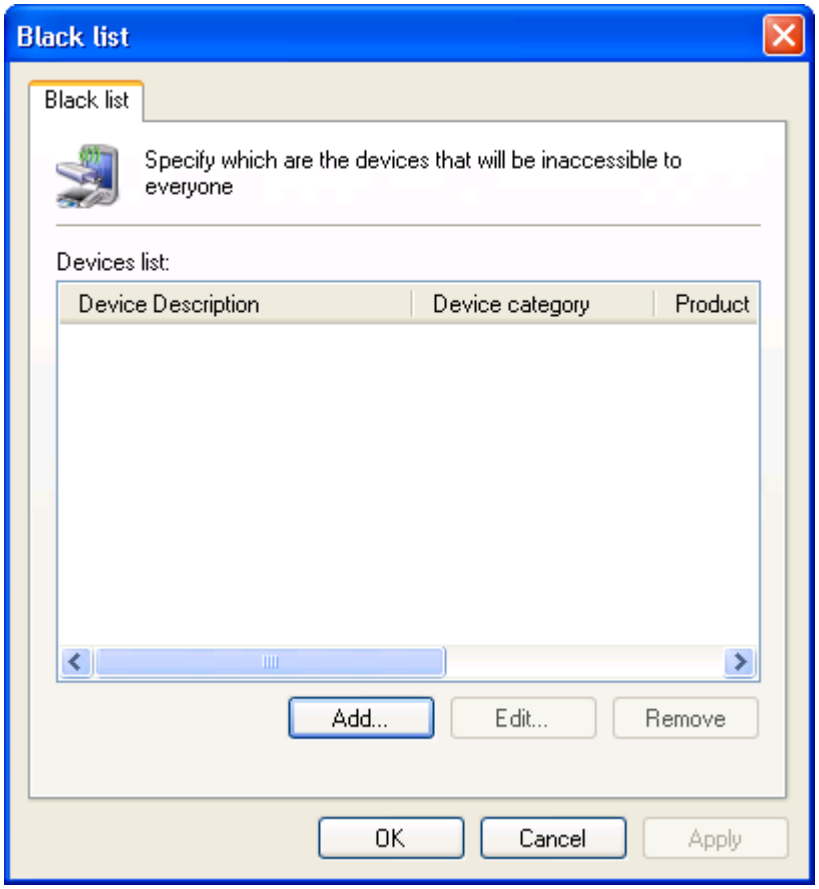
To add devices to the blacklist for a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

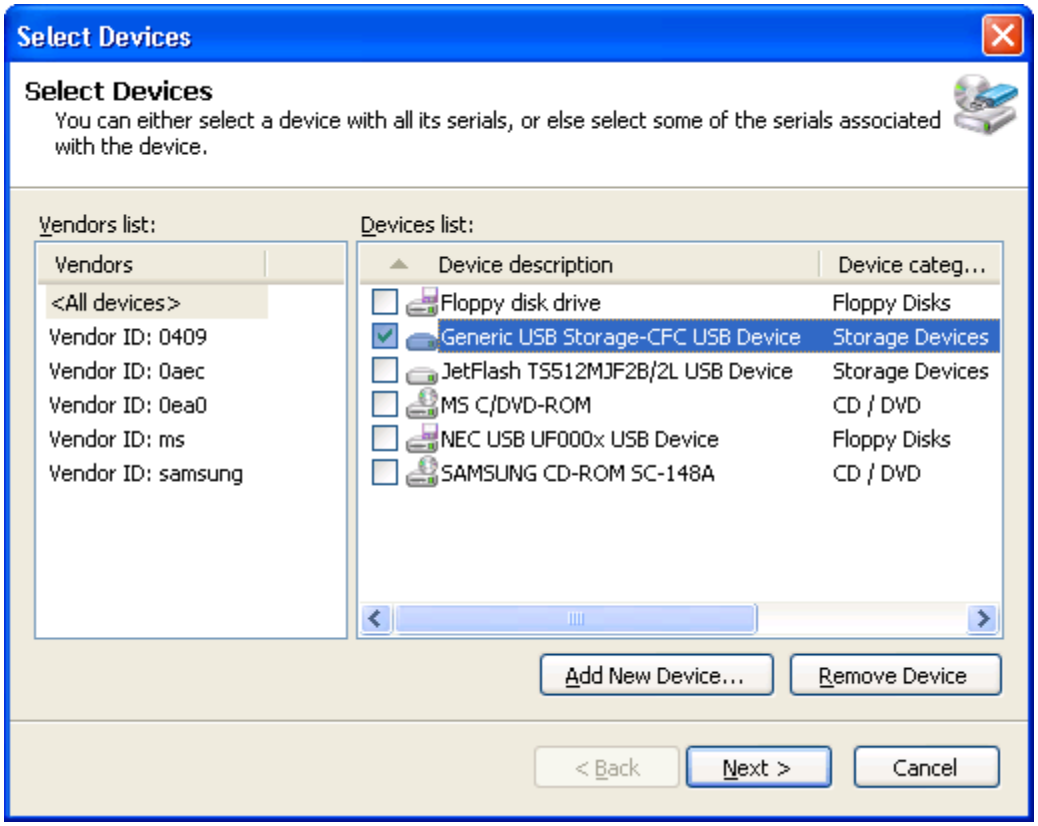
3. From the left pane, select the protection policy for which you want to blacklist devices.

4. From the right pane, click the **Devices Blacklist** hyperlink in the **Security** section.



Screenshot 77 - Black list options

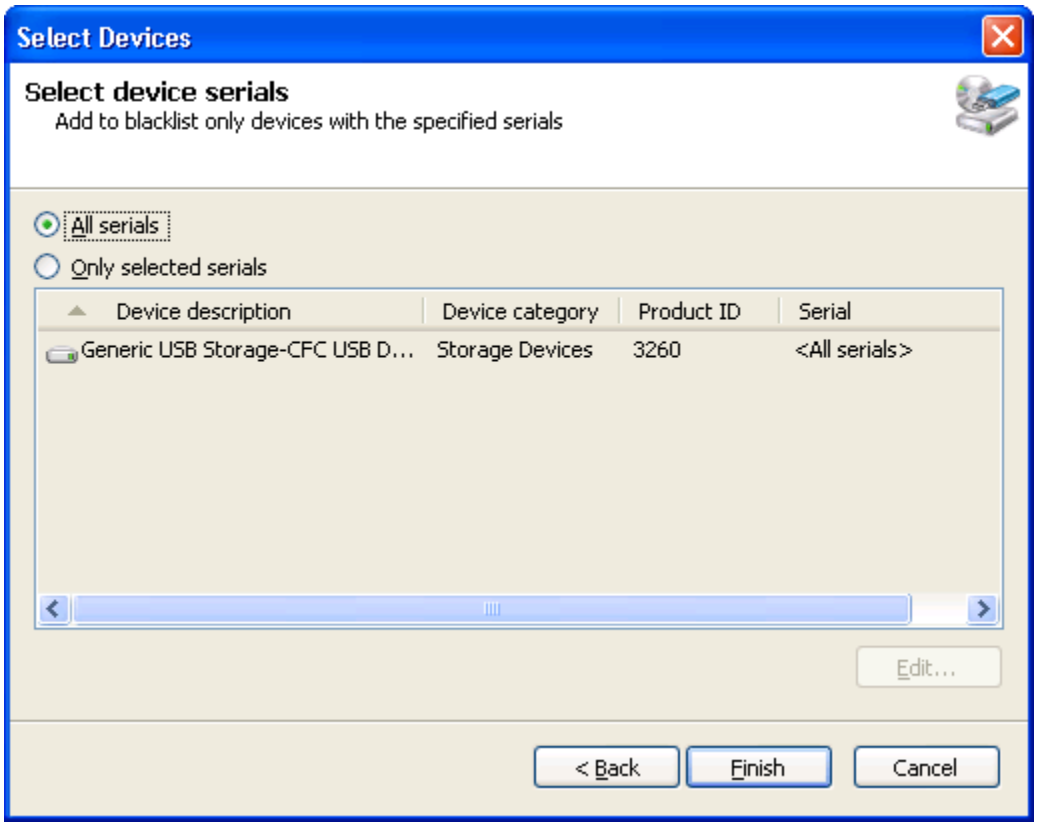
5. In the **Black list** dialog click **Add...** to select devices to add to the blacklist.



Screenshot 78 - Select Devices options

6. In the **Select Devices** dialog enable or disable the devices to add to the blacklist from the **Devices list**, , and click **Next**.

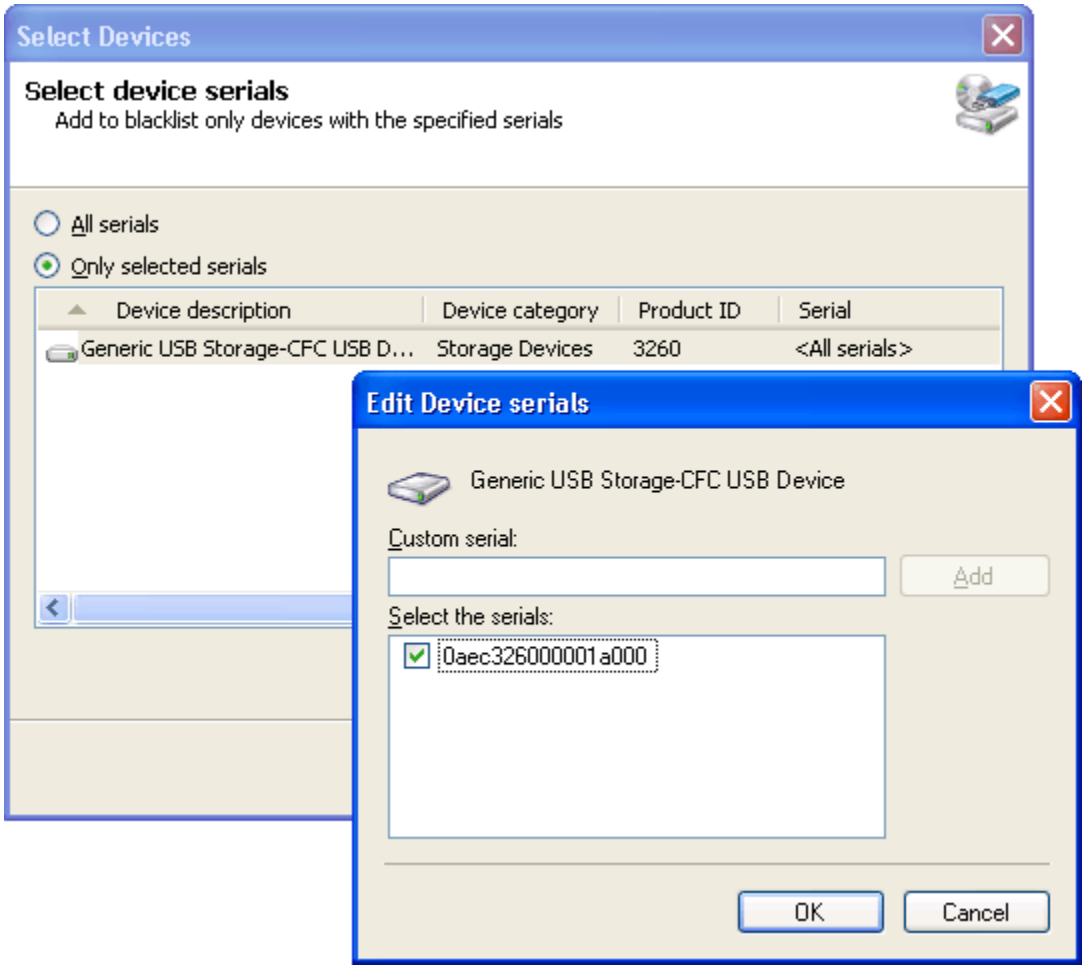
If a required device is not listed, click **Add New Device…** to specify the details of the device you want to add to the blacklist, and click **OK**.



Screenshot 79 - Select Devices options - Select device serials

7. Select the required serials related option from:

» **All serials** - to blacklist all serial numbers of a specific device. Click **Finish** and **OK**.



Screenshot 80 - Select Devices options - Edit Device serials

» **Only selected serials** - to specify that only particular device serial number(s) are to be added to the blacklist. Next, highlight the device and click **Edit…** to specify the serial number(s) to blacklist. Click **OK**, **Finish** and **OK**.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.11 Configuring device whitelist

GFI EndPointSecurity provides you with the facility to specify which device(s) can be made accessible to everyone. The whitelist is granular, so you can even whitelist a specific device with a specific serial number. You can do this on a policy by policy basis.

For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring whitelisted devices. For more information about the device scan feature, refer to the Discovering devices chapter in this manual.

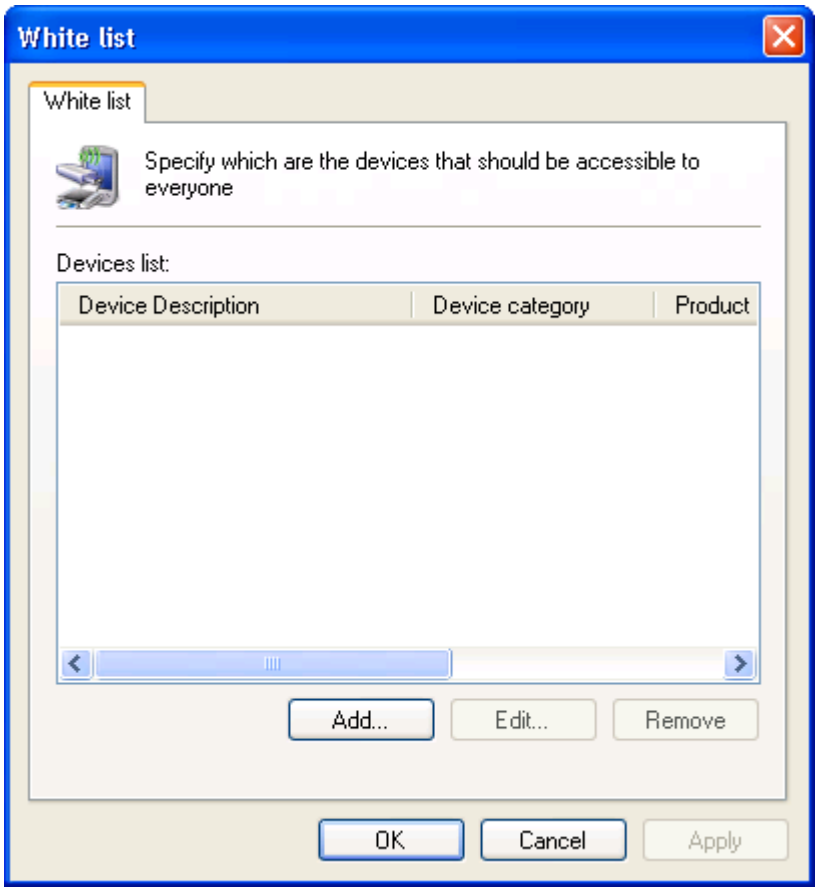
To add devices to the whitelist for a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

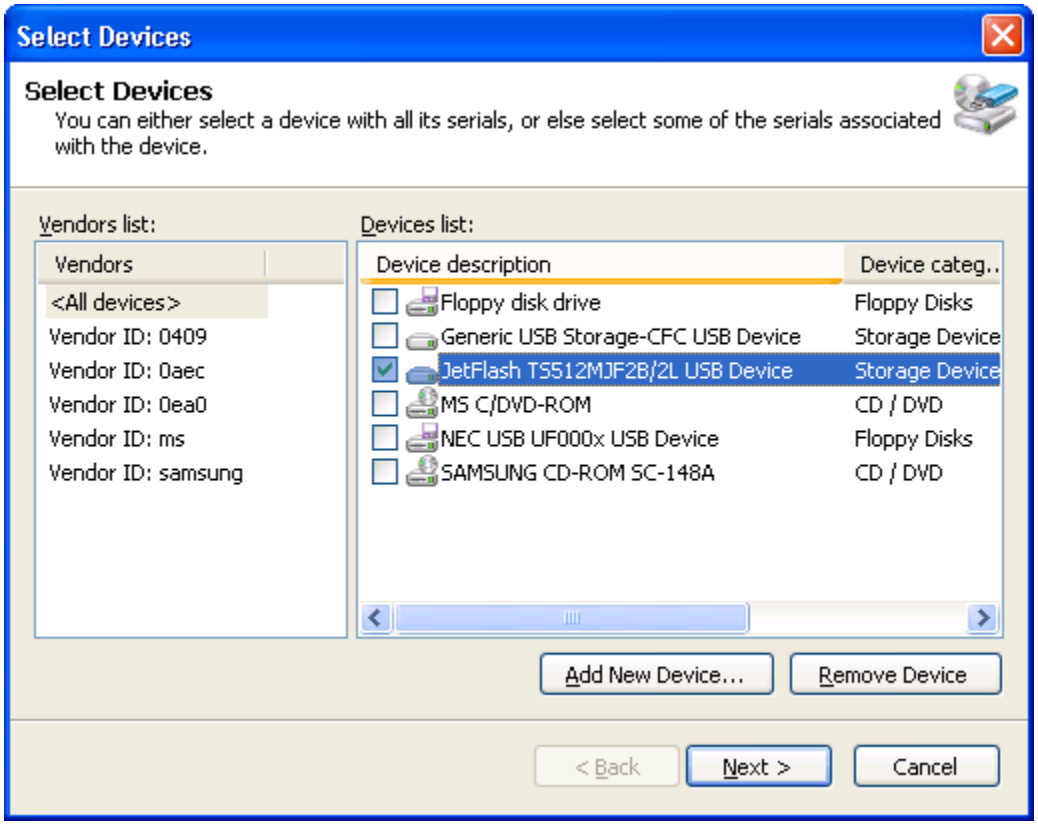
3. From the left pane, select the protection policy for which you want to whitelist devices.

4. From the right pane, click the **Devices WhiteList** hyperlink in the **Security** section.



Screenshot 81 - White list options

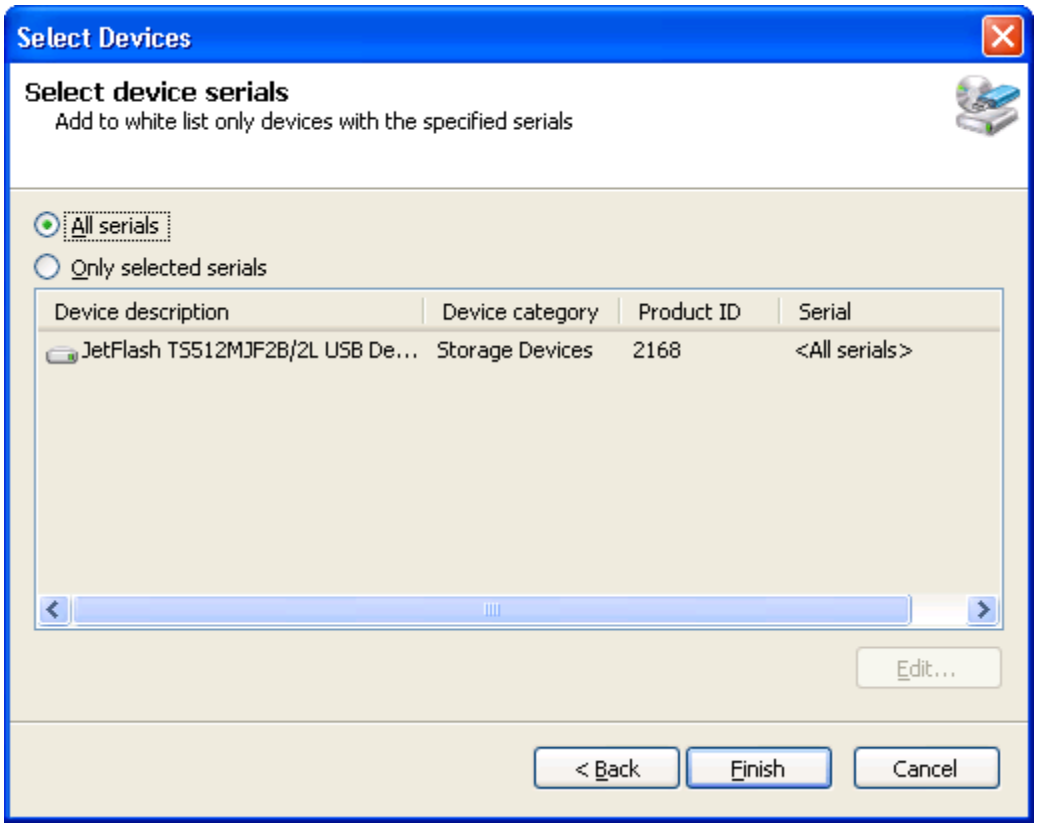
5. In the **White list** dialog click **Add...** to select devices to add to the whitelist.



Screenshot 82 - Select Devices options

6. In the **Select Devices** dialog enable or disable the devices to add to the whitelist from the **Devices list**, and click **Next**.

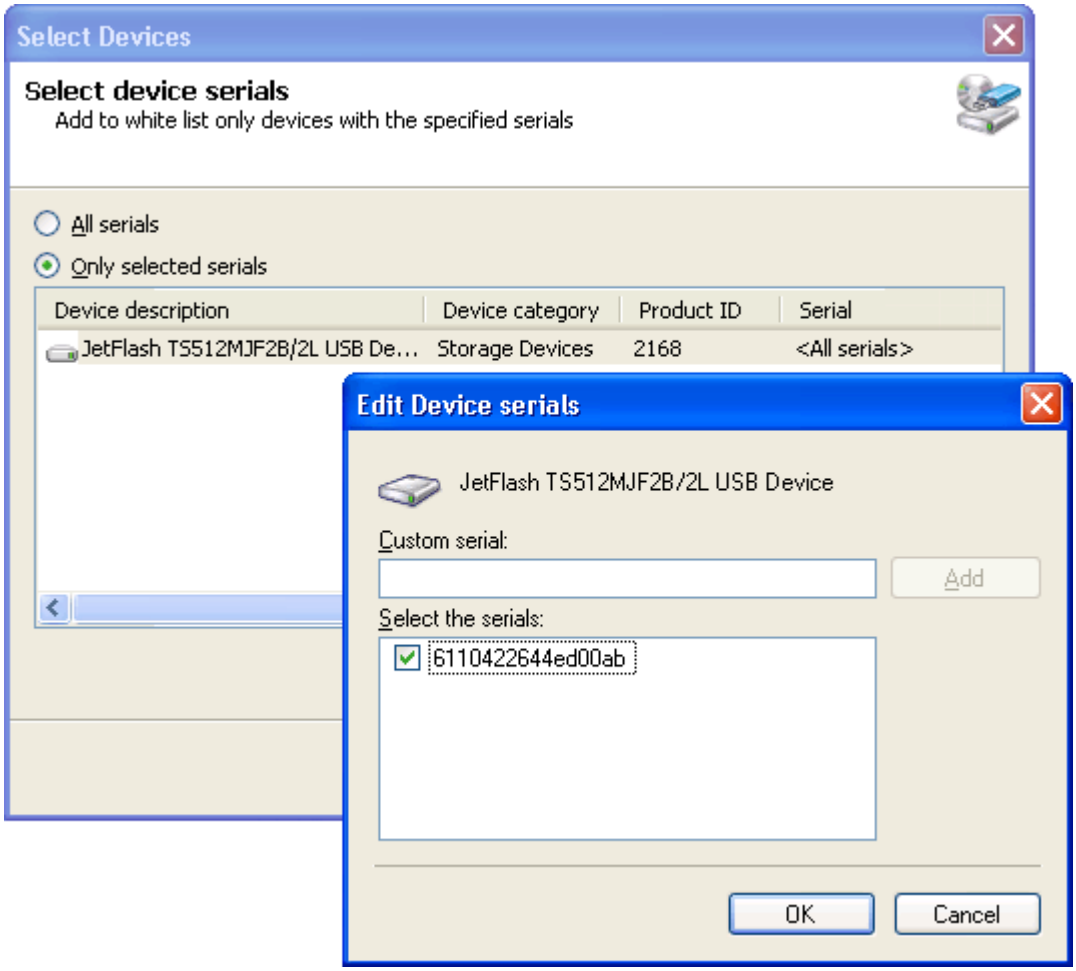
If a required device is not listed, click **Add New Device…** to specify the details of the device you want to add to the whitelist, and click **OK**.



Screenshot 83 - Select Devices options - Select device serials

7. Select the required serials related option from:

» **All serials** - to whitelist all serial numbers of a specific device. Click **Finish** and **OK**.



Screenshot 84 - Select Devices options - Edit Device serials

» **Only selected serials** - to specify that only particular device serial number(s) are to be added to the whitelist. Next, highlight the device and click **Edit…** to select the serial number(s) to whitelist. Click **OK**, **Finish** and **OK**.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.12 Configuring temporary access privileges

GFI EndPointSecurity provides you with the facility to grant temporary access to users, enabling them to access devices and connection ports (when such access is normally blocked) on protected target computers for a specified duration and time window. You can do this on a policy by policy basis.

When temporary access is granted, any permissions and settings (e.g. file-type filters) set in the protection policy applicable for the target computer, are temporarily overridden.

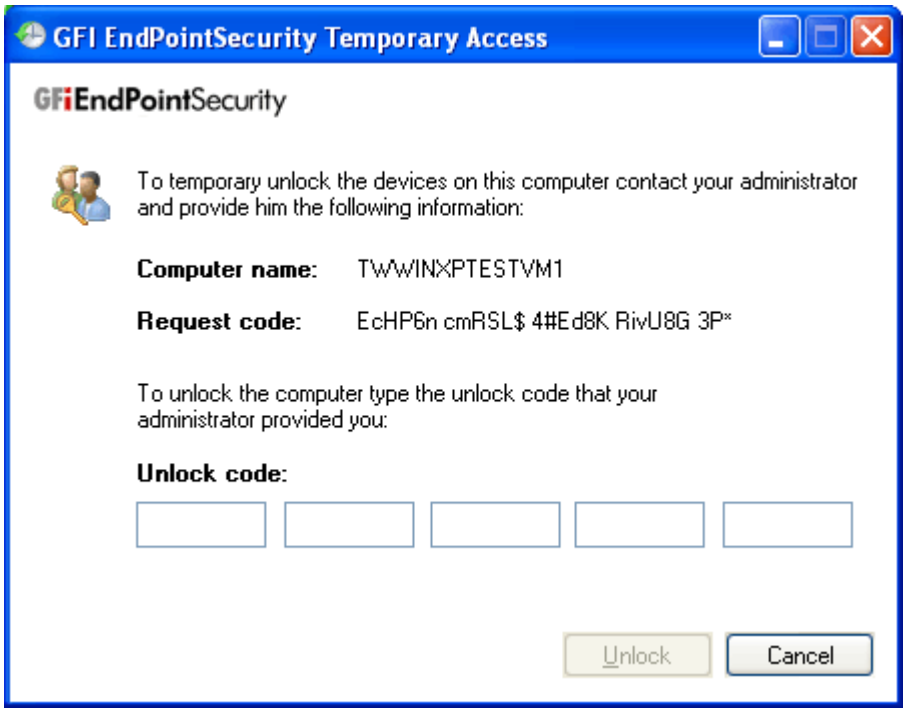
For more information on how temporary access requests and permissions work, refer to **How GFI EndPointSecurity works - Temporary access** section in the **About GFI EndPointSecurity** chapter.

9.12.1 Requesting temporary access for a protected computer

To generate a request code the user should launch the **GFI EndPointSecurity Temporary Access** tool:

Screenshot 85 - Devices Temporary Access icon

1. From the **Microsoft Windows Control Panel** click the **Devices Temporary Access** icon.


GFI EndPointSecurity Temporary Access
GFiEndPointSecurity
To temporary unlock the devices on this computer contact your administrator and provide him the following information:
Computer name: TWWINXPTESTVM1
Request code: EcHP6n cmRSL$ 4#Ed8K RivU8G 3P*
To unlock the computer type the unlock code that your administrator provided you:
Unlock code:
Unlock
Cancel

Screenshot 86 - GFI EndPointSecurity Temporary Access tool

2. In the **GFI EndPointSecurity Temporary Access** dialog take note of the **Request code** generated, and communicate the code together with the device type and/or connection port to be accessed, when, and for how long will device access be required to your security administrator.

Keep the **GFI EndPointSecurity Temporary Access** tool open.

3. When the administrator sends the unlock code, key it in the **Unlock code** field.

An unlock code keyed in on the protected target computer outside the specified validity period will not activate temporary access.

4. Click **Unlock** to activate temporary access. You are now able to access the required device and/or connection port.

9.12.2 Granting temporary access to a protected computer

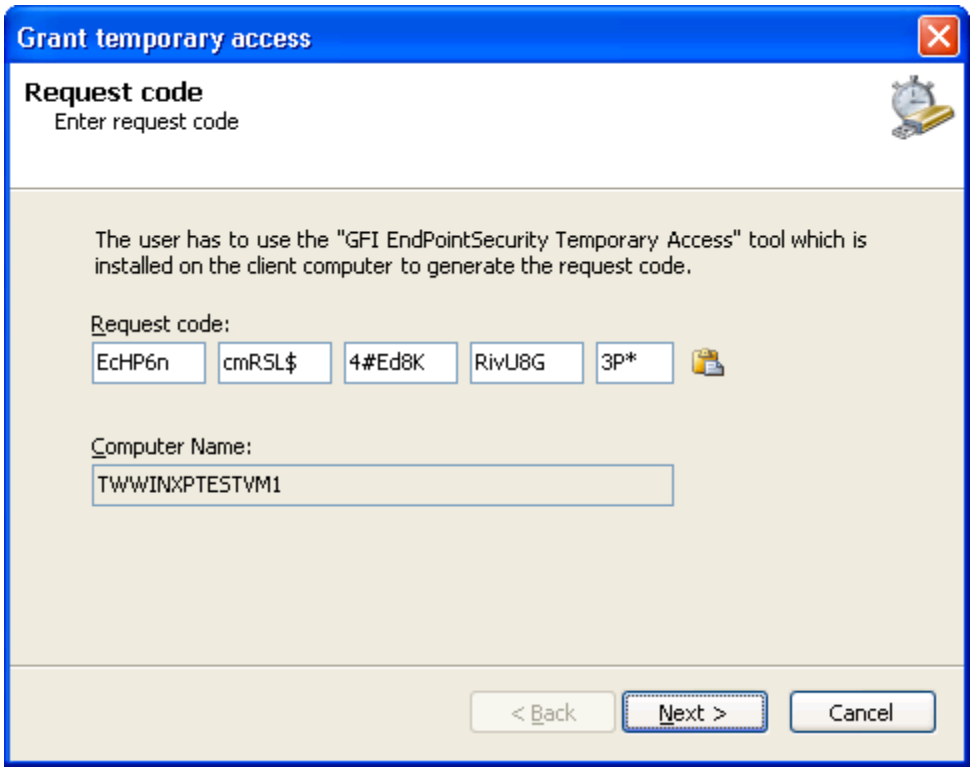
To grant temporary access the security administrator should:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

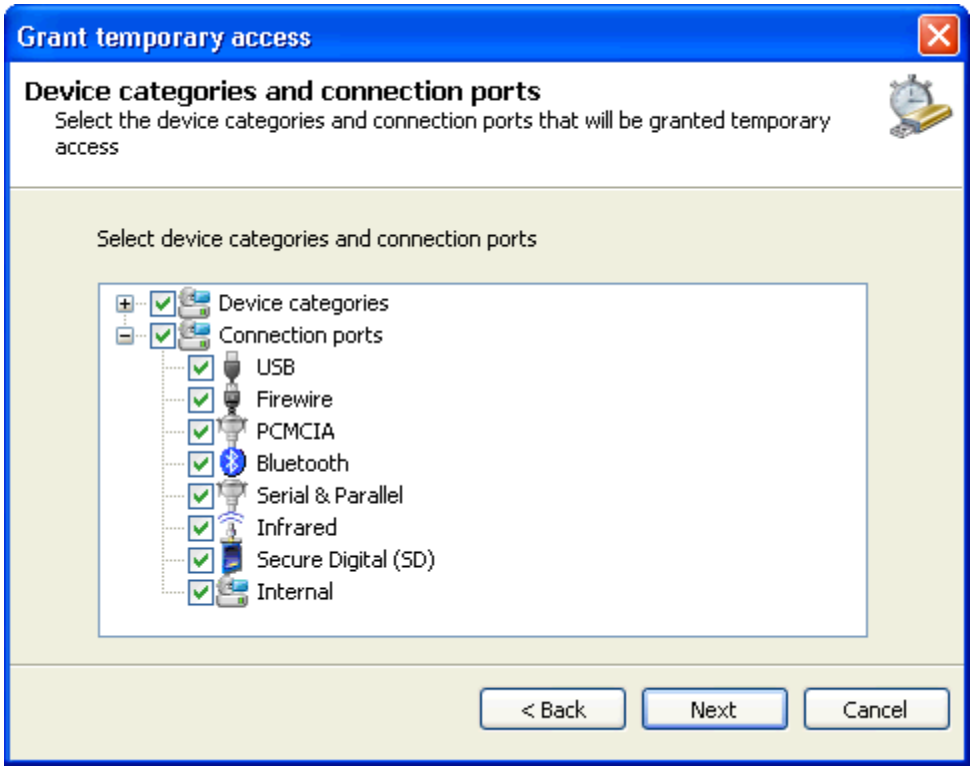
3. From the left pane, select the protection policy that includes the computer on which temporary access needs to be granted.

4. From the right pane, click the **Grant temporary access** hyperlink in the **Temporary Access** section.



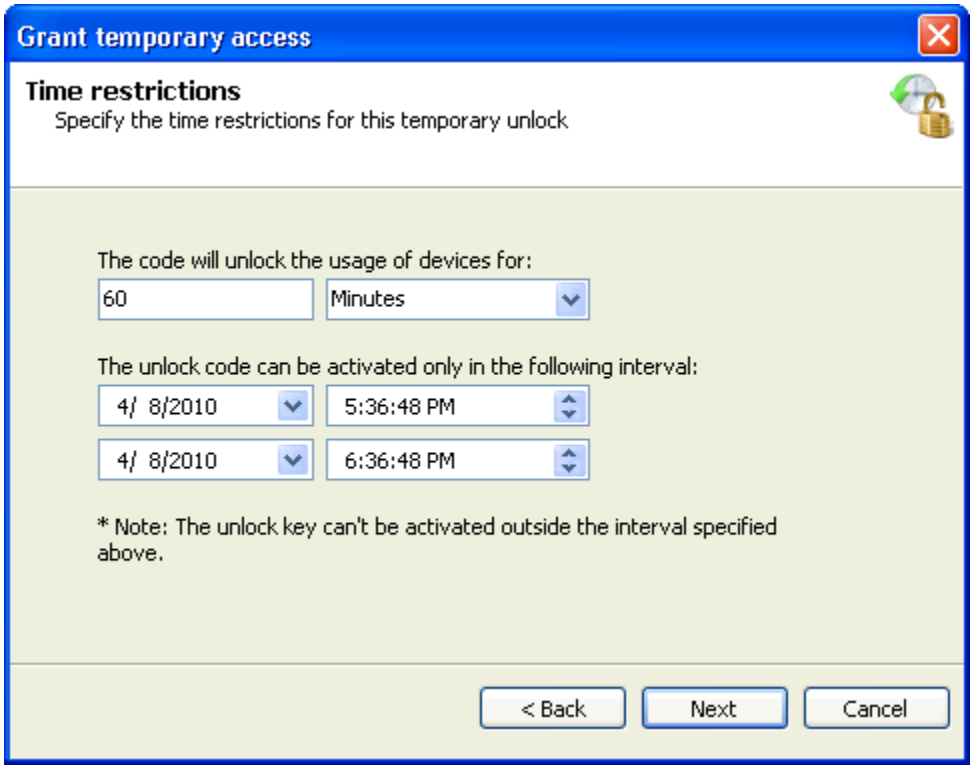
Screenshot 87 - Grant temporary access options - Request code

5. In the **Grant temporary access** dialog key in the request code received from the user, in the **Request code** field. The computer name from which the request code was generated is then displayed in the **Computer Name** field and click **Next**.



Screenshot 88 - Grant temporary access options - Device categories and connection ports

6. Enable the required device categories and/or connection ports from the list, to which you will be granting temporary access, and click **Next**.


Grant temporary access
Time restrictions
Specify the time restrictions for this temporary unlock
The code will unlock the usage of devices for:
60
Minutes
The unlock code can be activated only in the following interval:
4/ 8/2010
5:36:48 PM
4/ 8/2010
6:36:48 PM
* Note: The unlock key can't be activated outside the interval specified above.
< Back
Next
Cancel

Screenshot 89 - Grant temporary access options - Time restrictions

7. Specify the duration during which access is allowed, and the validity period of the unlock code, and click **Next**.

8. Take note of the **Unlock code** generated, and communicate the code to the user requesting temporary access and click **Finish**.

9.13 Configuring file-type filters

GFI EndPointSecurity provides you with the facility to specify file-type restrictions on files, such as .DOC or .XLS files, being copied to/from allowed devices. You can apply these restrictions to Active Directory (AD) users and/or user groups, or local users and/or groups schema. You can do this on a policy by policy basis.

Filtering is based on file extension checks and real file type signature checks. Real file type signature checking can be done on the following file types:

AVI	BMP	CAB	CHM	DLL	DOC	EMF	EXE
GIF	HLP	HTM	JPE	JPEG	JPG	LNK	M4A
MDB	MP3	MPEG	MPG	MSG	MSI	OCX	P7M
PDF	PPT	RAR	RTF	SCR	SYS	TIF	TIFF
TXT	URL	WAV	XLS	ZIP			

For any other file type not specified above, filtering is based only on the file extension.

File-type filtering is only applied to device categories and/or ports for which permissions have been set to allow access.

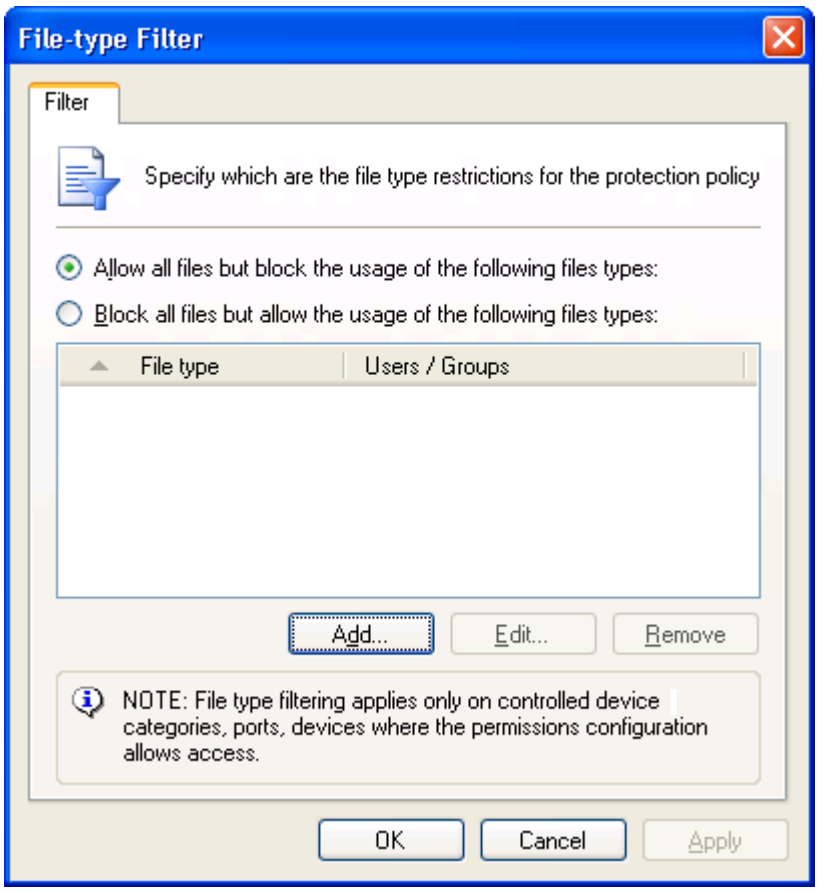
To configure file-type restrictions for users within a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy for which you want to specify file-type restrictions.

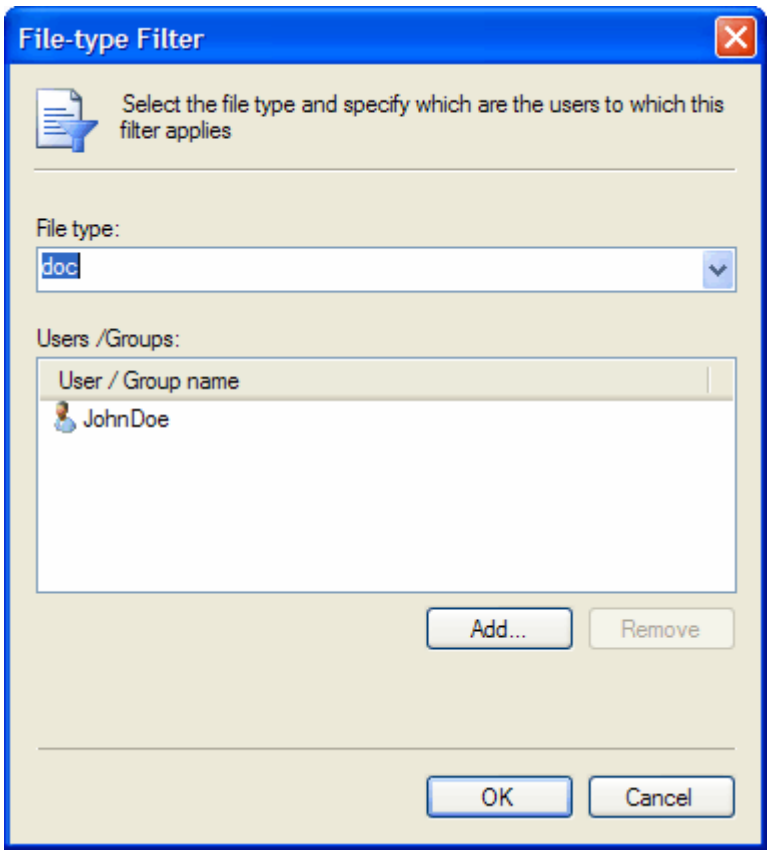
4. From the right pane, click the **File-type Filter** hyperlink in the **File control** section.


File-type Filter
Filter
Specify which are the file type restrictions for the protection policy
Allow all files but block the usage of the following files types:
Block all files but allow the usage of the following files types:
File type
Users / Groups
Add...
Edit...
Remove
NOTE: File type filtering applies only on controlled device categories, ports, devices where the permissions configuration allows access.
OK
Cancel
Apply

Screenshot 90 - File-type Filter options

5. In the **File-type Filter** dialog select the restriction to apply to this policy:

- » Allow all files but block the usage of the following file types
- » Block all files but allow the usage of the following file types



Screenshot 91 - File-type Filter and user options

6. Click **Add…** and select or key in the file-type from the **File type** dropdown list.

7. Click **Add…** to specify the user(s)/group(s) who are allowed/blocked from accessing the specified file-type, and click **OK**.

Repeat the preceding 2 sub-steps for each file type to restrict.

8. Click **OK** twice.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.14 Configuring security encryption

GFI EndPointSecurity provides you with the facility to allow or block Active Directory (AD) users and/or user groups, or local users and/or groups schema from accessing specific file-types stored on devices that are encrypted with BitLocker To Go, a Microsoft Windows 7 feature. These restrictions are applied when the encrypted devices are connected to the target computers covered by the protection policy.

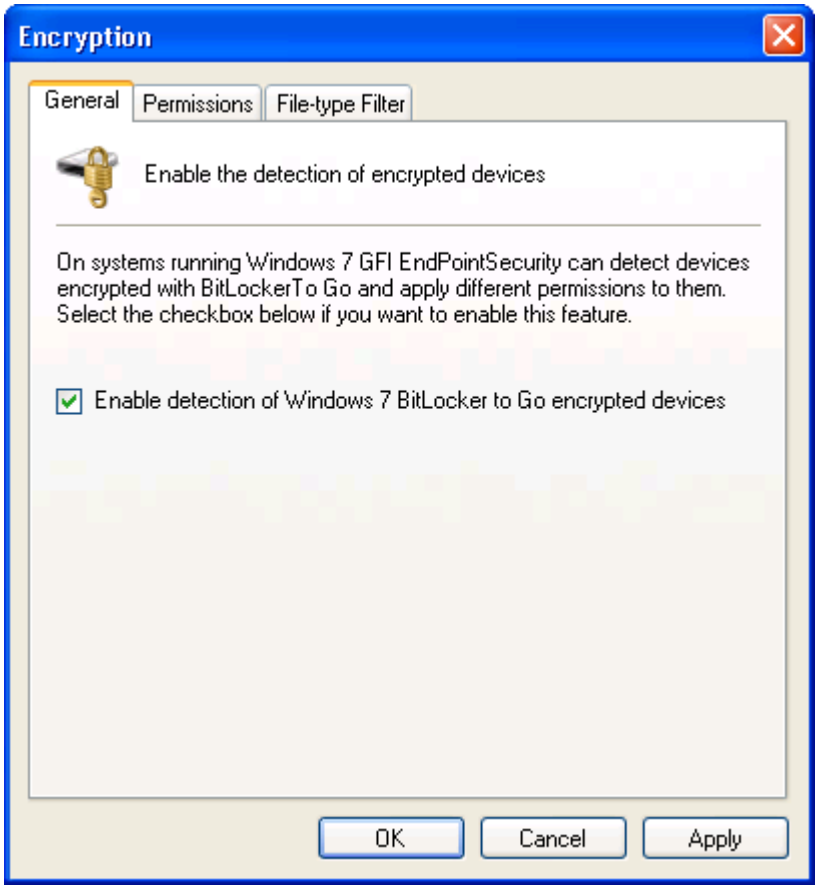
To configure restrictions for devices that are encrypted with BitLocker To Go within a specific protection policy:

1. From the GFI EndPointSecurity management console, click the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

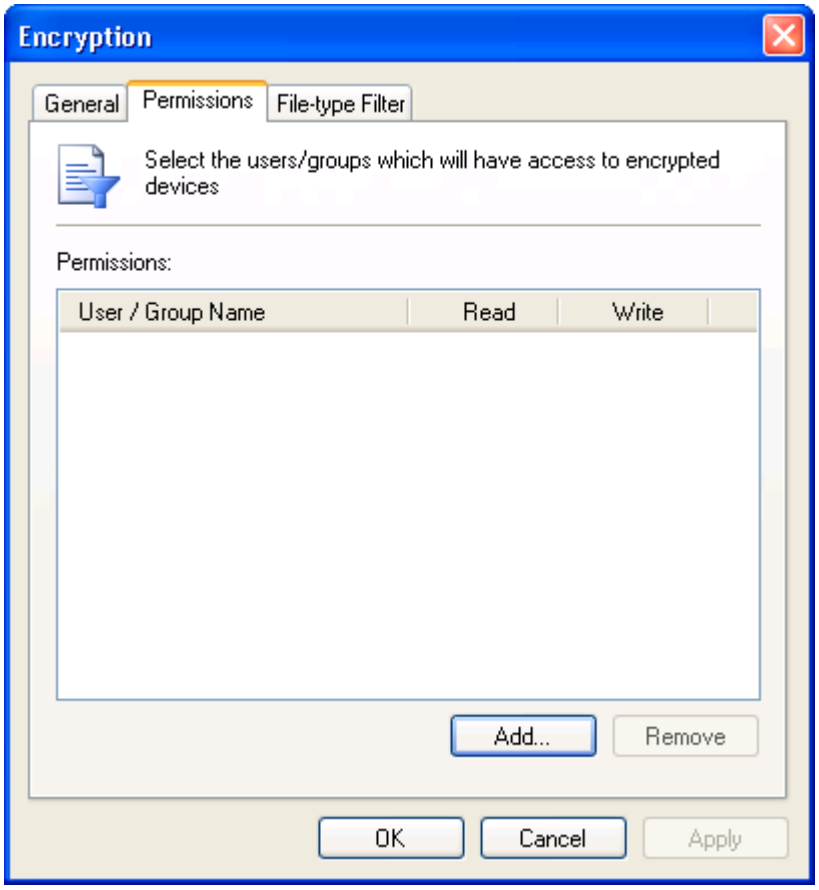
3. From the left pane, select the protection policy for which you want to specify file-type restrictions.

4. From the right pane, click the **Encryption** hyperlink in the **Security** section.


Encryption
General
Permissions
File-type Filter
Enable the detection of encrypted devices
On systems running Windows 7 GFI EndPointSecurity can detect devices encrypted with BitLockerTo Go and apply different permissions to them. Select the checkbox below if you want to enable this feature.
Enable detection of Windows 7 BitLocker to Go encrypted devices
OK
Cancel
Apply

Screenshot 92 - Encryption options - General tab

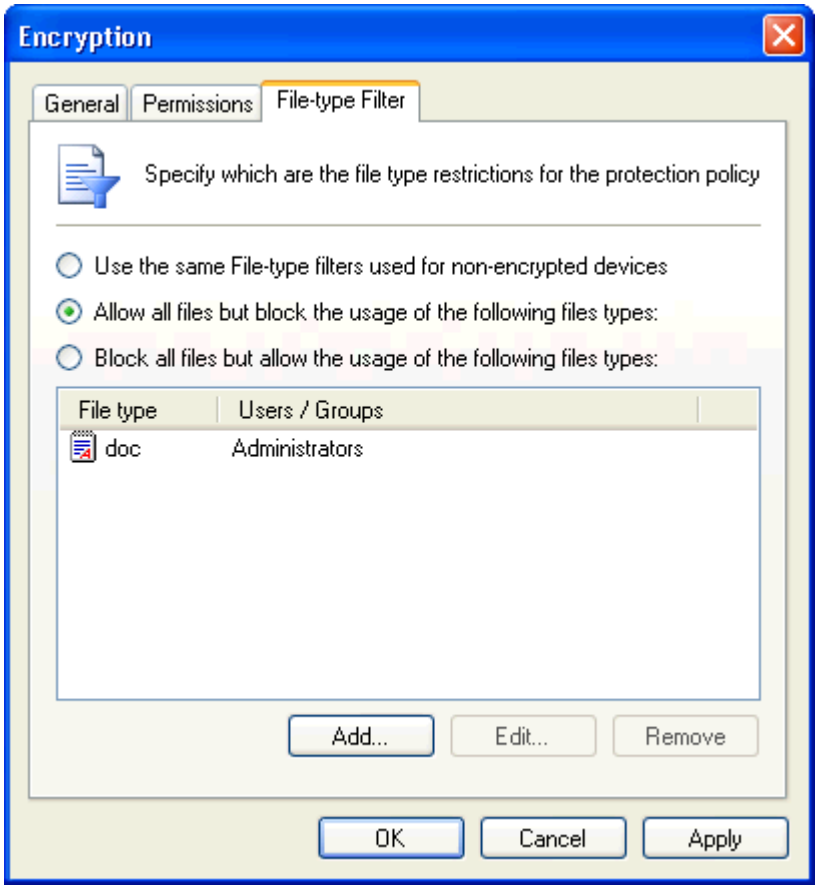
5. In the **Encryption** dialog select the **General** tab and enable or disable **Enable detection of Windows 7 BitLocker To Go encrypted devices** to allow or block the usage of devices that are encrypted with BitLocker To Go.



Screenshot 93 - Encryption options - Permissions tab

6. If the BitLocker To Go option is enabled, select the **Permissions** tab.

7. Click **Add…** to specify the user(s)/group(s) that will have access to the encrypted devices detected by this protection policy, and click **OK**.



Screenshot 94 - Encryption options - File-type Filter tab

8. If the BitLocker To Go option is enabled, select the **File-type Filter** tab to configure the file-types that are to be restricted access.

9. Select the restriction to apply to this policy:

- Use the same File-type filters used for non-encrypted devices
- Allow all files but block the usage of the following file types
- Block all files but allow the usage of the following file types

10. For the last 2 options, click **Add…** and select or key in the file-type from the **File type** dropdown list.

11. Click **Add…** to specify the user(s)/group(s) who are allowed/blocked from accessing the specified file-type, and click **OK**.

Repeat the preceding 2 sub-steps for each file type to restrict.

12. Click **OK** twice.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.15 Configuring event logging

GFI EndPointSecurity agents record events related to attempts made to access devices and connection ports on target computers. The agents also record events related to service operations. You can specify where these events are to be stored, and also what types of events are to be logged. You can do this on a policy by policy basis.

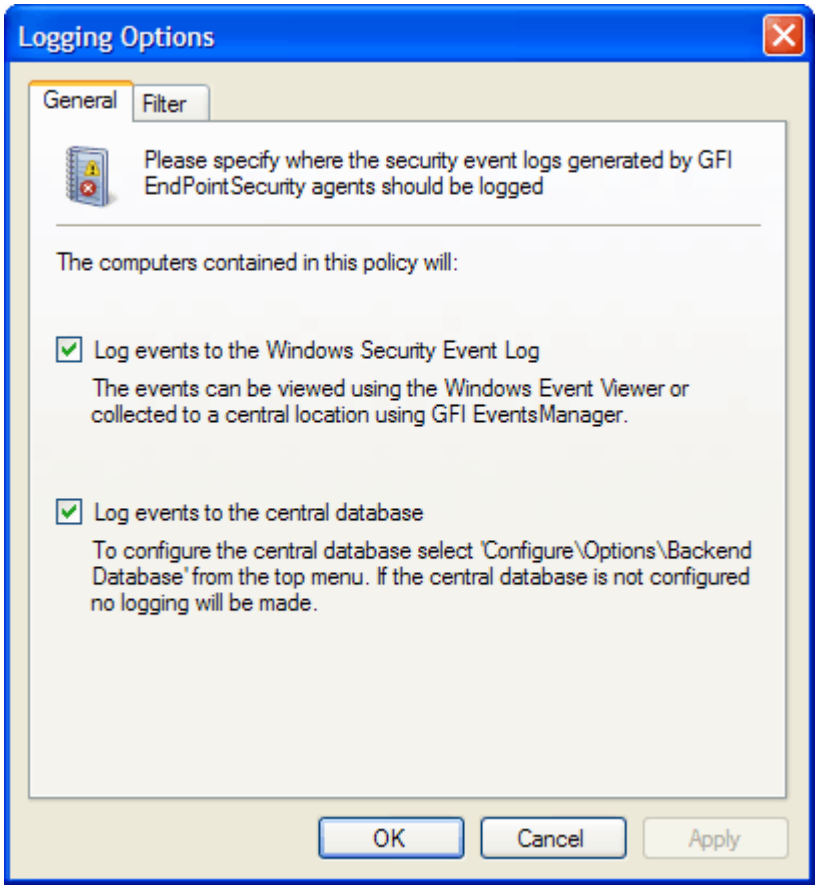
To specify logging options for users within a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy for which you want to specify logging options.

4. From the right pane, click the **Set Logging Options** hyperlink in the **Logging and Alerting** section.


Logging Options
General
Filter
Please specify where the security event logs generated by GFI EndPointSecurity agents should be logged
The computers contained in this policy will:
Log events to the Windows Security Event Log
The events can be viewed using the Windows Event Viewer or collected to a central location using GFI EventsManager.
Log events to the central database
To configure the central database select 'Configure\Options\Backend Database' from the top menu. If the central database is not configured no logging will be made.
OK
Cancel
Apply

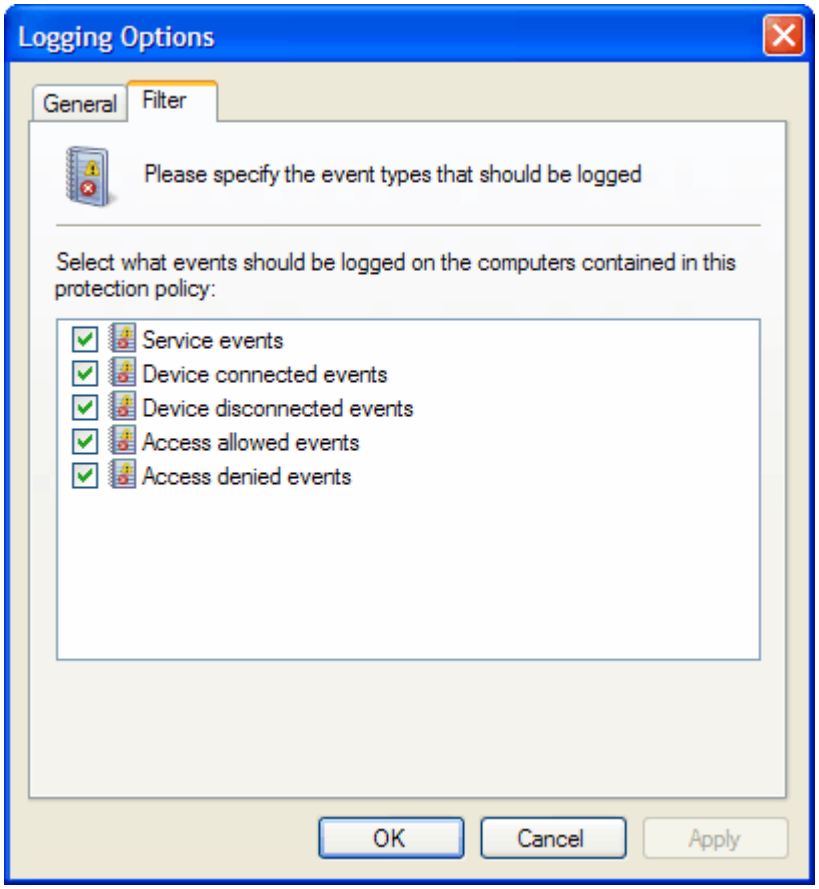
Screenshot 95 - Logging Options - General tab

5. In the **Logging Options** dialog select the **General** tab.

6. Enable or disable the locations where to store events generated by this protection policy:

- **Log events to the Windows Security Event Log** - you can view events through the Windows Event Viewer of every target computer or through GFI EventsManager after they are collected in a central location.
- **Log events to the central database** - you can view the events within the Logs Browser sub-tab in the GFI EndPointSecurity management console. This option requires the configuration of a central database. For more information on how to configure a central database, refer to the **Configuring database backend** section in the **Customizing GFI EndPointSecurity** chapter.

If both options are enabled, then the same data is logged in both locations.



Screenshot 96 - Logging Options - Filter tab

7. Select the **Filter** tab, select any of the following event types that are to be logged by this protection policy and click **OK**:

- Service events
- Device connected events
- Device disconnected events
- Access allowed events
- Access denied events.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.16 Configuring alerts

GFI EndPointSecurity can be configured to send alerts to specified recipients when particular events are generated. You can configure alerts to be sent through several alerting options, and also specify the types of events for which alerts are to be sent. You can do this on a policy by policy basis.

Alert recipients are not Active Directory (AD) users and/or user groups, or local users and/or groups schema, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts. It is best to create alert recipients prior to configuring alerts. For more information on how to create the users and groups for notification purposes, refer to the **Configuring alert recipients** section in the **Customizing GFI EndPointSecurity** chapter.

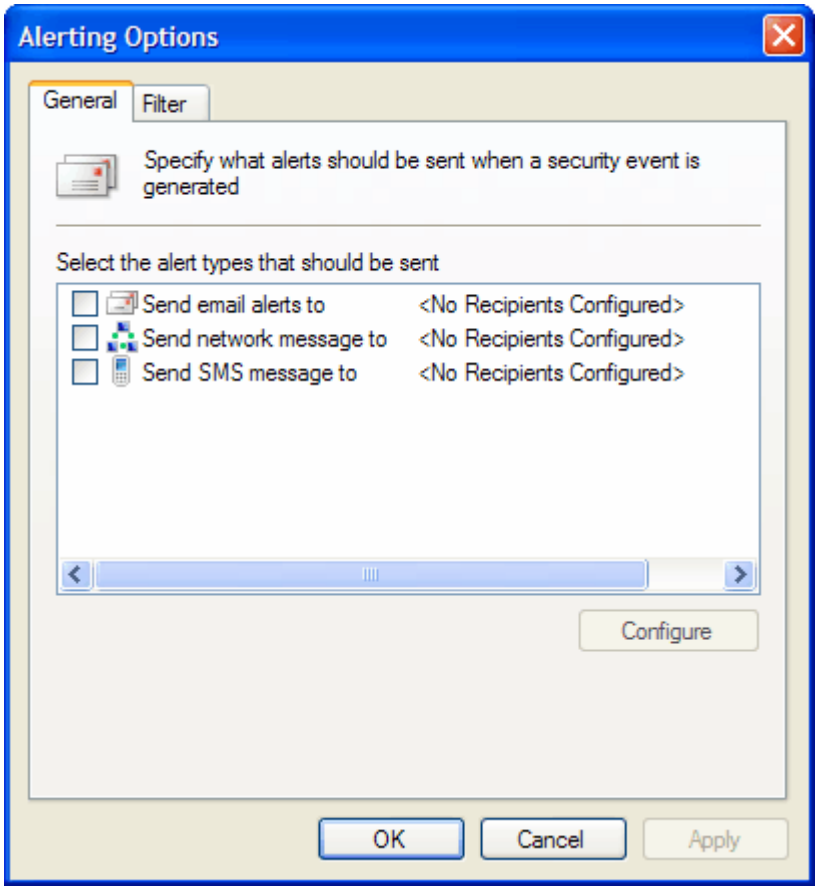
To specify alerting options for users within a specific protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy for which you want to specify notification options.

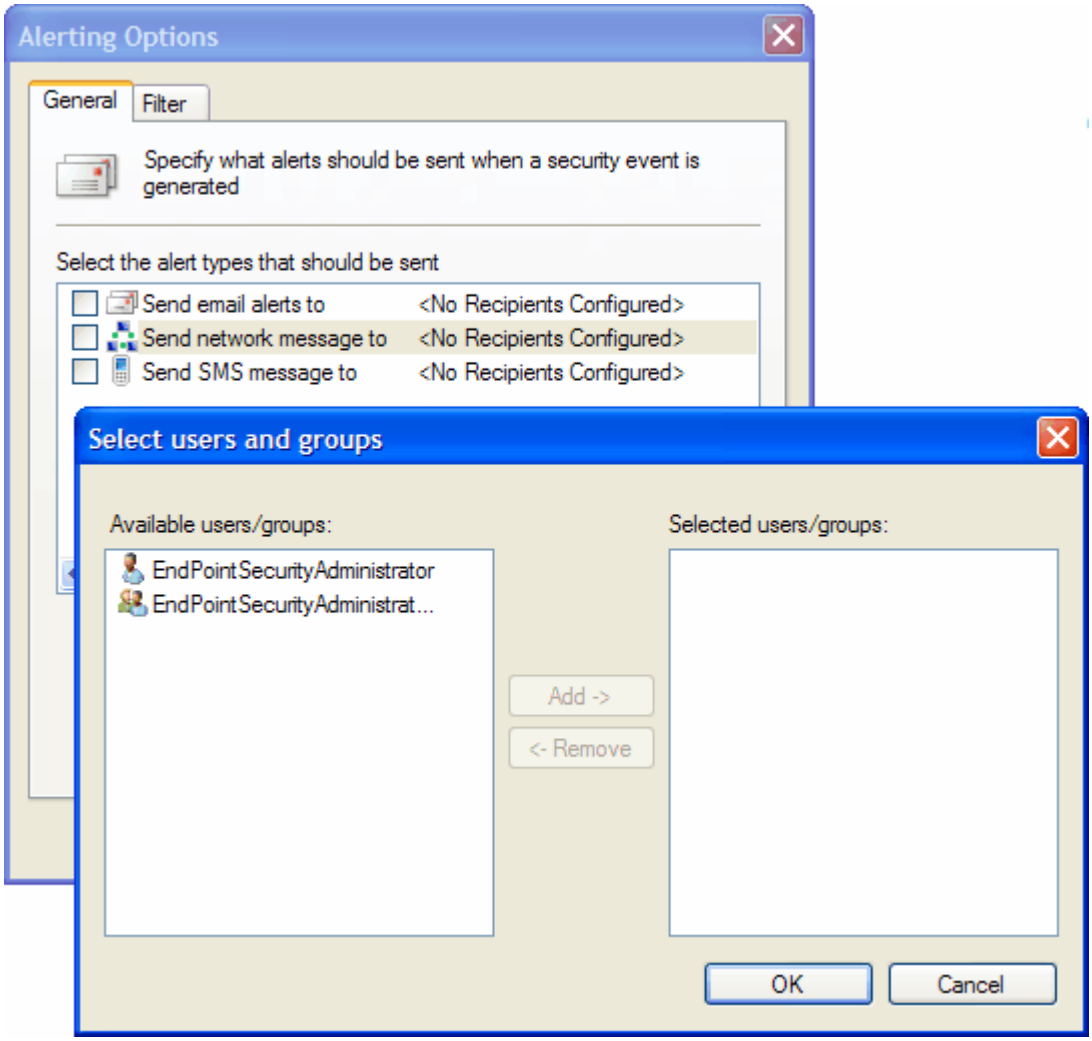
4. From the right pane, click the **Alerting options** hyperlink in the **Logging and Alerting** section.



Screenshot 97 - Alerting Options - General tab

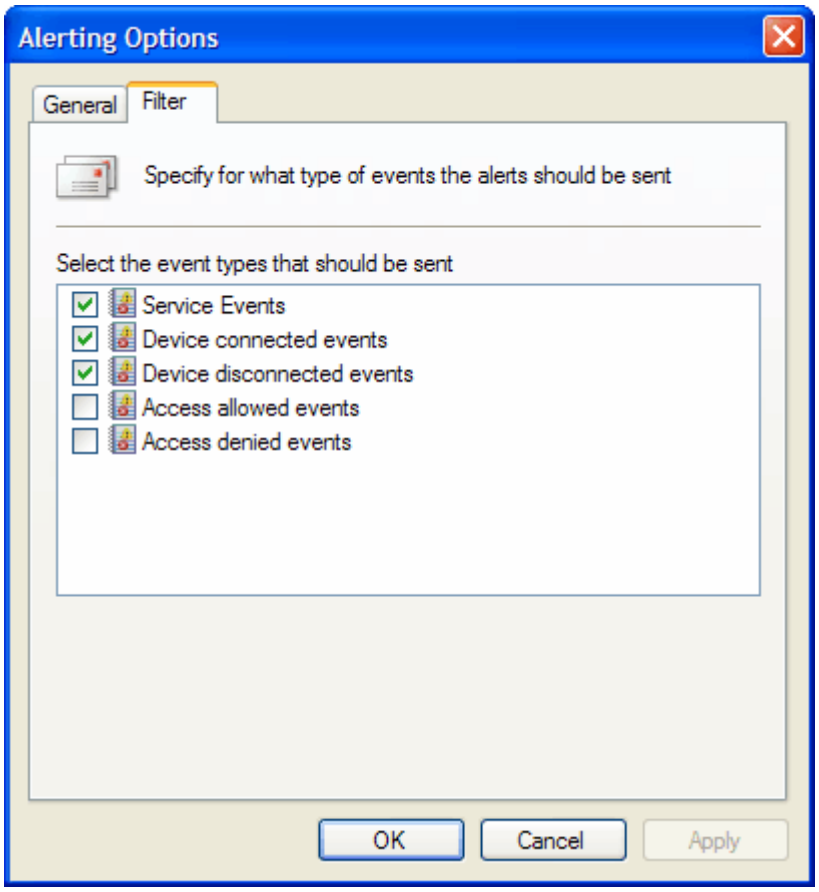
5. In the **Alerting Options** dialog, select the **General** tab and select any of the following alert types to be sent to alert recipients:

- Email alerts
- Network messages
- SMS messages.



Screenshot 98 - Alerting Options - Configuring users and groups

6. For each alert type enabled, highlight the alert type and click **Configure** to specify the user(s)/group(s) to whom the alert should be sent and click **OK**.



Screenshot 99 - Alerting Options - Filter tab

7. Select the **Filter** tab, select any of the following event types for which alerts are to be sent by this protection policy and click **OK**:

- Service events
- Device connected events
- Device disconnected events
- Access allowed events
- Access denied events.

To deploy the protection policy updates on to the target computers specified in the policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Deploy to all computers…** hyperlink in the **Common tasks** section.

9.17 Setting a policy as the default policy

GFI EndPointSecurity provides you with the facility to define the protection policy that is assigned to newly discovered network computers by the agent deployment feature. You can do this on a policy by policy basis.

By default:

- the agent deployment feature is set to use the **General Control** protection policy (shipping default protection policy), but you can elect any other protection policy as the default policy.

To elect another protection policy as the default protection policy:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Protection Policies** sub-tab.

3. From the left pane, select the protection policy that you want to elect as the default policy.
4. From the left pane, click the **Set as default policy** hyperlink in the **Common tasks** section.

10 Customizing GFI EndPointSecurity

10.1 Introduction

All settings within GFI EndPointSecurity are fully customizable and can be configured to suit your company's needs. In this chapter you will learn how to:

- Configure auto discovery settings
- Configure the alerts administrator account
- Configure alerting options
- Configure alert recipients
- Configure groups of alert recipients
- Configure digest report
- Configure database backend
- Configure user messages
- Configure advanced options.

10.2 Configuring auto discovery settings

GFI EndPointSecurity provides you with the facility to search for newly connected computers to the network at configured scheduled times through the auto discovery feature and to configure the following auto discovery settings:

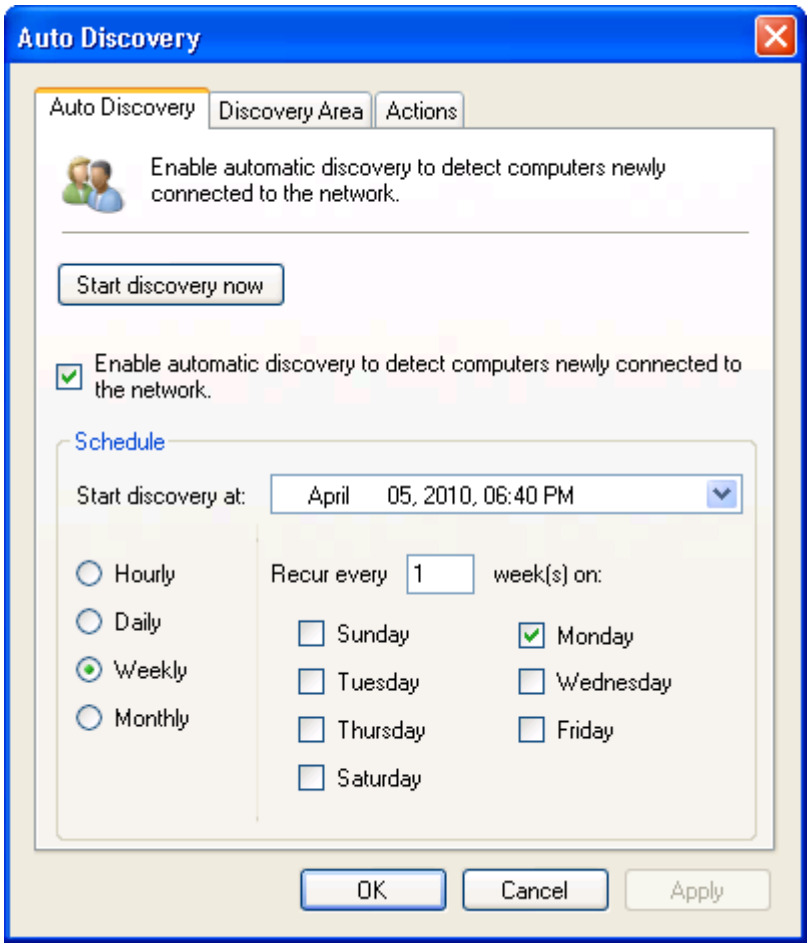
- The frequency and schedule of the searches
- The discovery area covered
- The policy assigned to newly discovered target computers and the logon credentials.
- By default:
- the auto discovery settings are set to scan the **Current domain/workgroup**
- the install agents settings are set to assign the **General Control** protection policy (shipping default protection policy) on to the newly discovered computers.

To configure the Auto Discovery settings:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.

3. From the left pane, click the **Auto discovery settings…** hyperlink in the **Common Tasks** section.



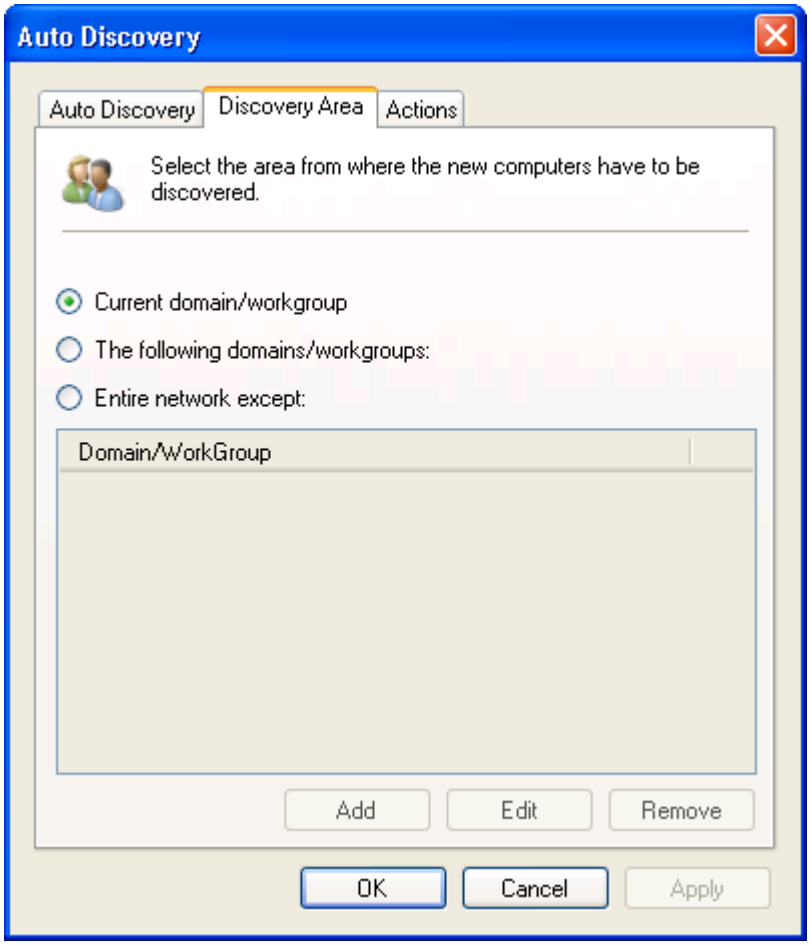
Screenshot 100 - Auto Discovery options - Auto Discovery tab

4. In the **Auto Discovery** dialog select the **Auto Discovery** tab.

5. Click **Start discovery now** to run the auto discovery feature now.

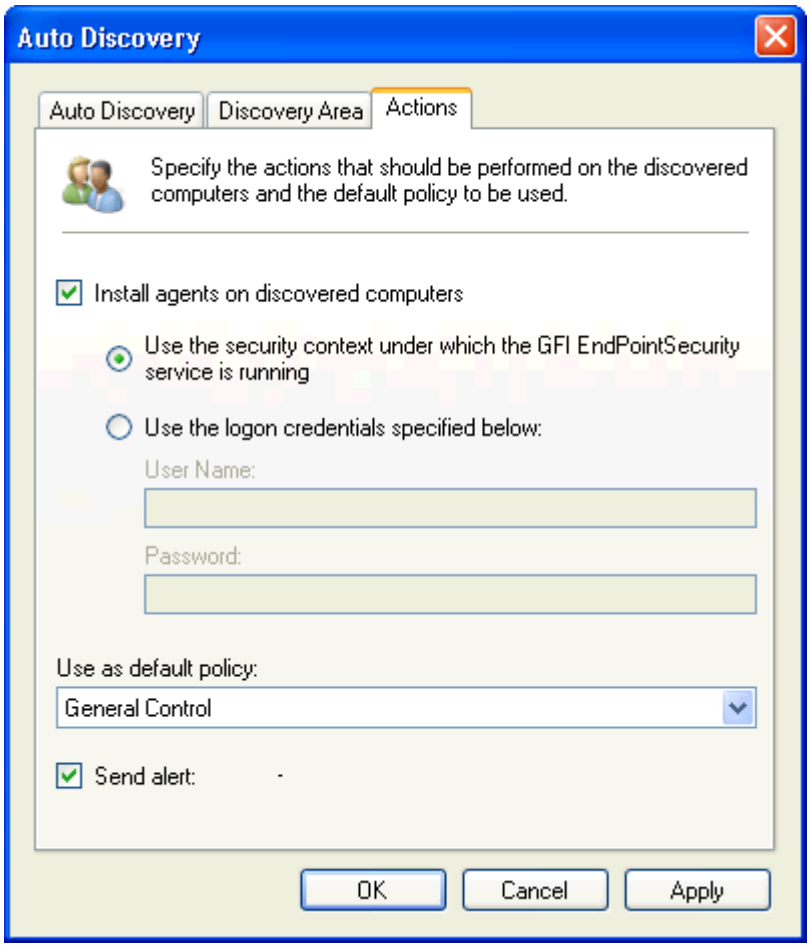
6. Enable or disable the **Enable automatic discovery to detect computers newly connected to the network** checkbox.

7. In the **Schedule** section select the start date and set frequency of the searches from **Hourly**, **Daily**, **Weekly** or **Monthly**.



Screenshot 101 - Auto Discovery options - Discovery Area tab

8. Select the **Discovery Area** tab and select the area to be covered by the discovery feature. For **The following domains/workgroups** and **Entire network except** click **Add** and key in the **Domain/workgroup name**.



Screenshot 102 - Auto Discovery options - Actions tab

9. Select the **Actions** tab and enable or disable **Install agents on discovered computers.** If enabled, click **Yes** to confirm the enabling of the Automatic Protection feature. Select the logon credentials that GFI EndPointSecurity requires to physically log on to the target computer(s).

By default, GFI EndPointSecurity is configured to use the logon credentials of the currently logged-on user account from which GFI EndPointSecurity application is running.

10. Select the protection policy from the drop-down list to be automatically applied to newly discovered target computers.

11. Enable or disable **Send alert**, and click **OK**.

10.3 Configuring the alerts administrator account

GFI EndPointSecurity provides you with the facility to configure profile accounts to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages. Upon installation, GFI EndPointSecurity automatically creates an alerts administrator account without the following contact details:

- Contact details including email address and phone number
- The typical working hours
- The type of alert(s) to send during and outside working hours
- The notification group that the user belongs to.

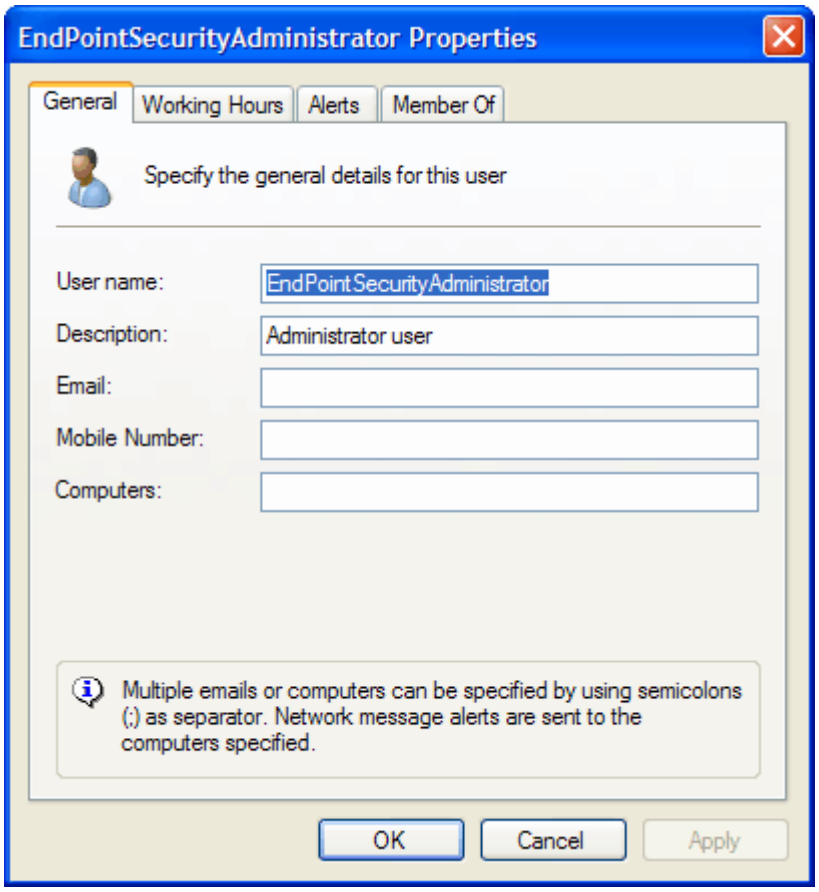
Alert administrators are not Active Directory (AD) users and/or user groups, or local users and/or groups schema.

By default:

- GFI EndPointSecurity will automatically create the **EndPointSecurityAdministrator** account (for alerts purposes) upon installation and sets it as a member of the **EndPointSecurityAdministrators** notification group.

To configure the GFI EndPointSecurityAdministrator account:

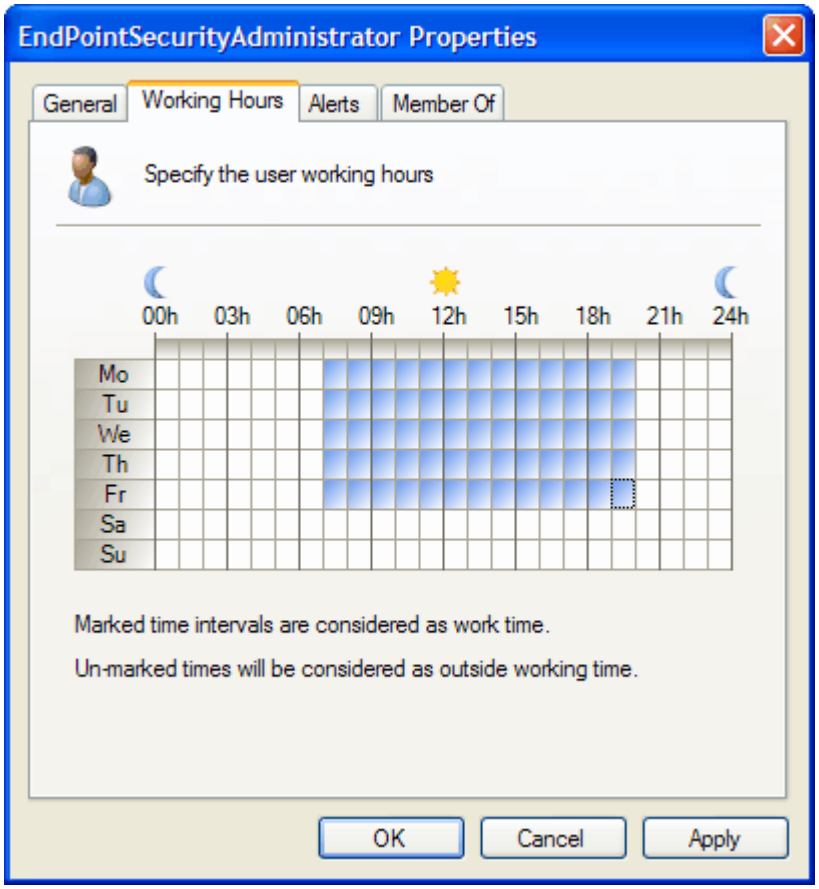
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. Click on the **Users** sub-node.
5. From the right pane, highlight the **EndPointSecurityAdministrator** account.
6. From the left pane, click the **Edit selected user…** hyperlink in the **Actions** section.



Screenshot 103 - EndPointSecurityAdministrator Properties options - General tab

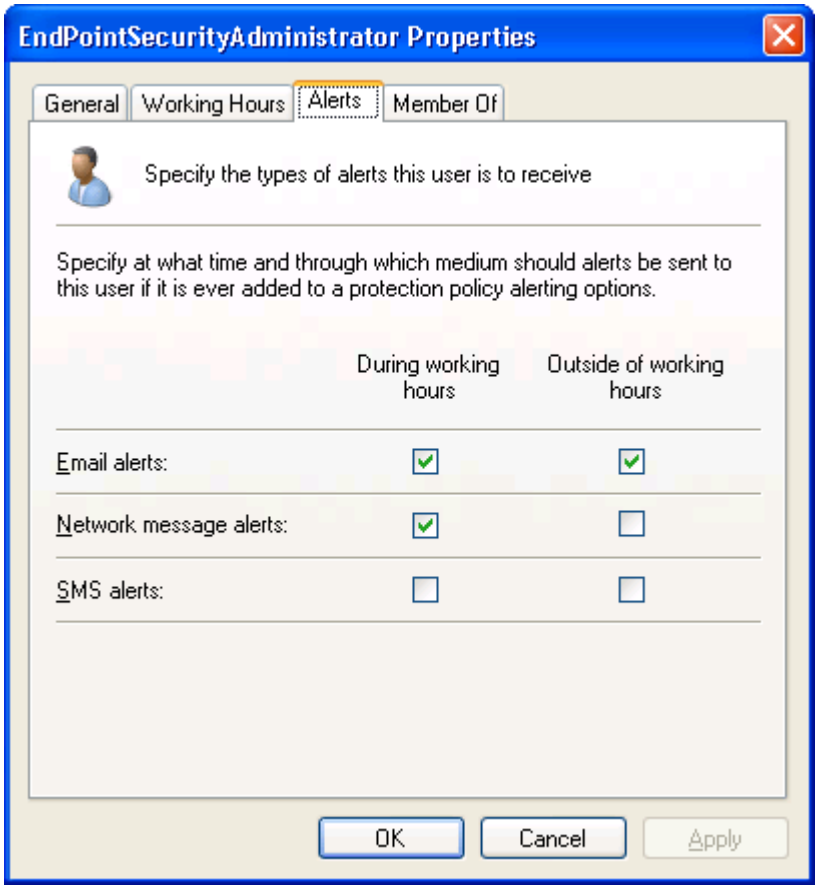
7. In the **EndPointSecurityAdministrator Properties** dialog select the **General** tab and key in the contact details such as email addresses, mobile number and computer names/IP addresses (for network message alerts addressed to the administrator) as required.

More than one email address and more than one computer name/IP address can be specified. Separate entries with semicolons ';'.



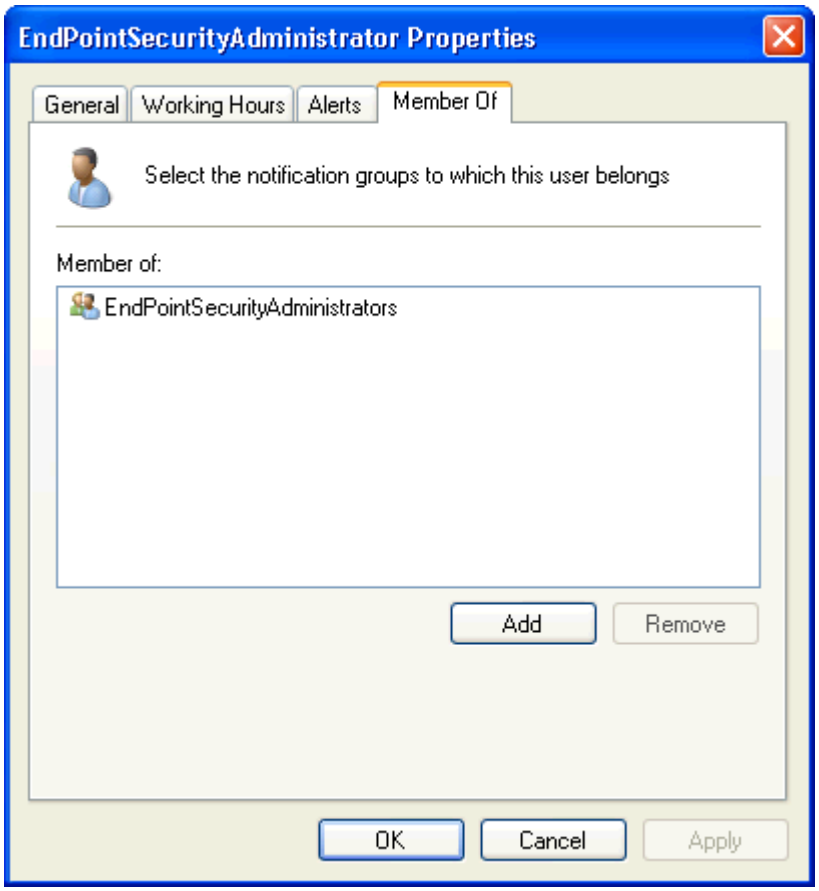
Screenshot 104 - EndPointSecurityAdministrator Properties options - Working Hours tab

8. Select the **Working Hours** tab and mark the typical working hours of the user.


EndPointSecurityAdministrator Properties
General
Working Hours
Alerts
Member Of
Specify the types of alerts this user is to receive
Specify at what time and through which medium should alerts be sent to this user if it is ever added to a protection policy alerting options.
During working hours
Outside of working hours
Email alerts:
Network message alerts:
SMS alerts:
OK
Cancel
Apply

Screenshot 105 - EndPointSecurityAdministrator Properties options - Alerts tab

9. Select the **Alerts** tab and enable that the types of alerts that will be sent during and outside of the marked working hours.



Screenshot 106 - EndPointSecurityAdministrator Properties options - Member Of tab

10. Select the **Member Of** tab.

11. Click **Add** to select the notification group(s) that this user belongs to, and click **OK**.

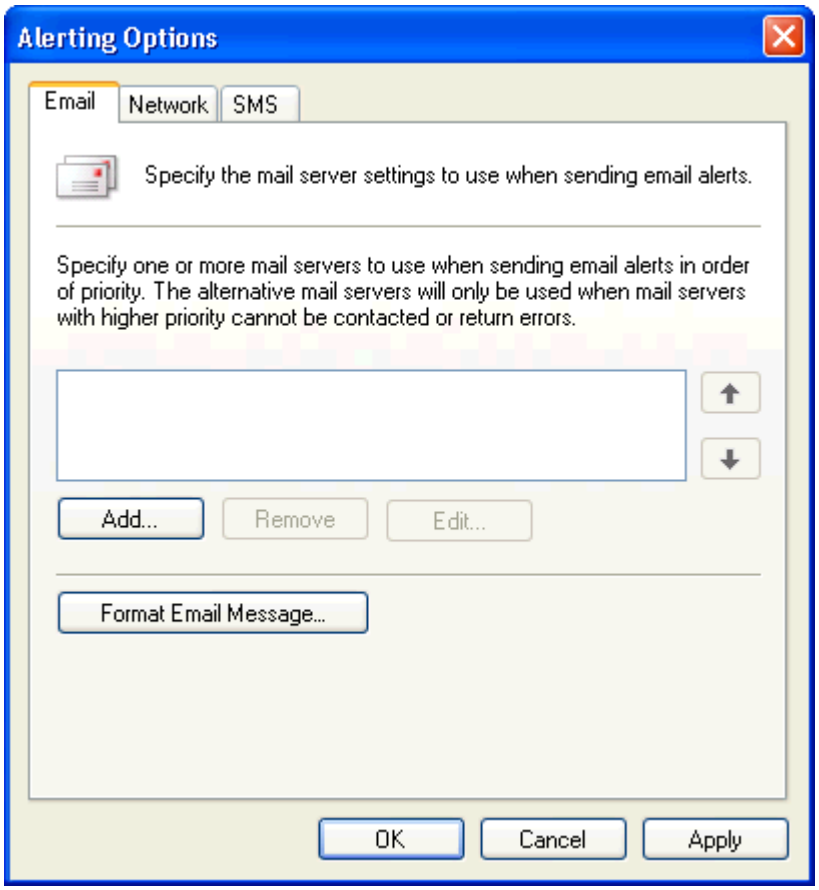
10.4 Configuring alerting options

GFI EndPointSecurity allows you configure the following alerting options:

- The mail server settings, sender details and email message that will be used to send email alerts
- The network message to use when sending network alerts
- The SMS gateway and SMS message that will be used to send alerts by SMS

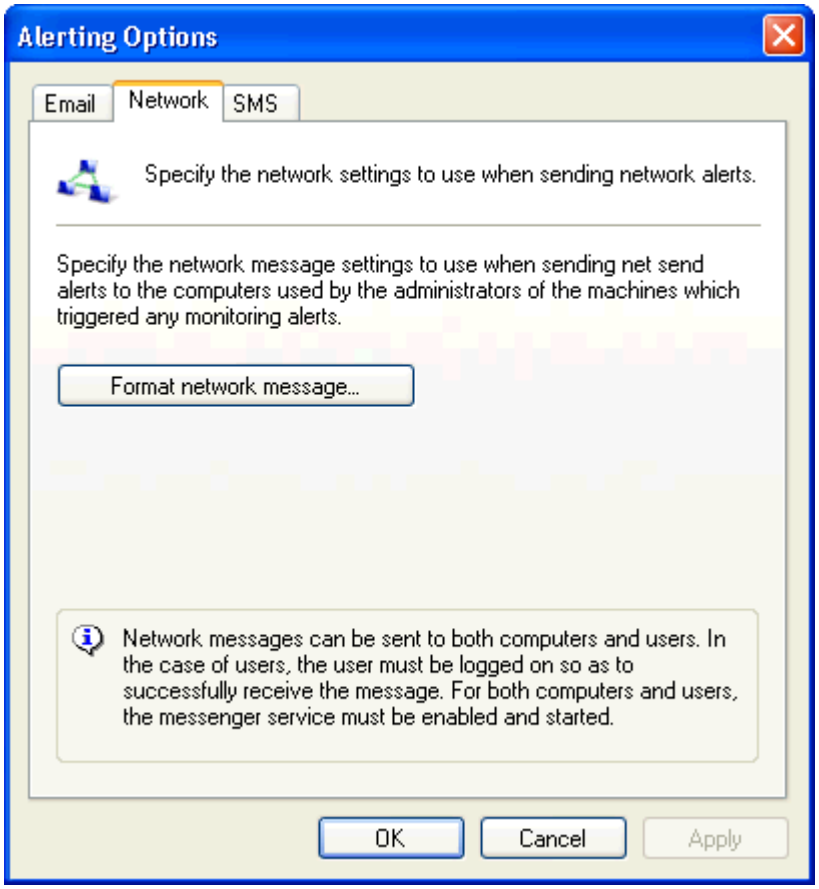
To configure the general alerting parameters:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. From the right pane, click the **Edit alerting options** hyperlink in the **Alerting Options** section.


Alerting Options
Email
Network
SMS
Specify the mail server settings to use when sending email alerts.
Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.
Add...
Remove
Edit...
Format Email Message...
OK
Cancel
Apply

Screenshot 107 - Alerting Options - Email tab

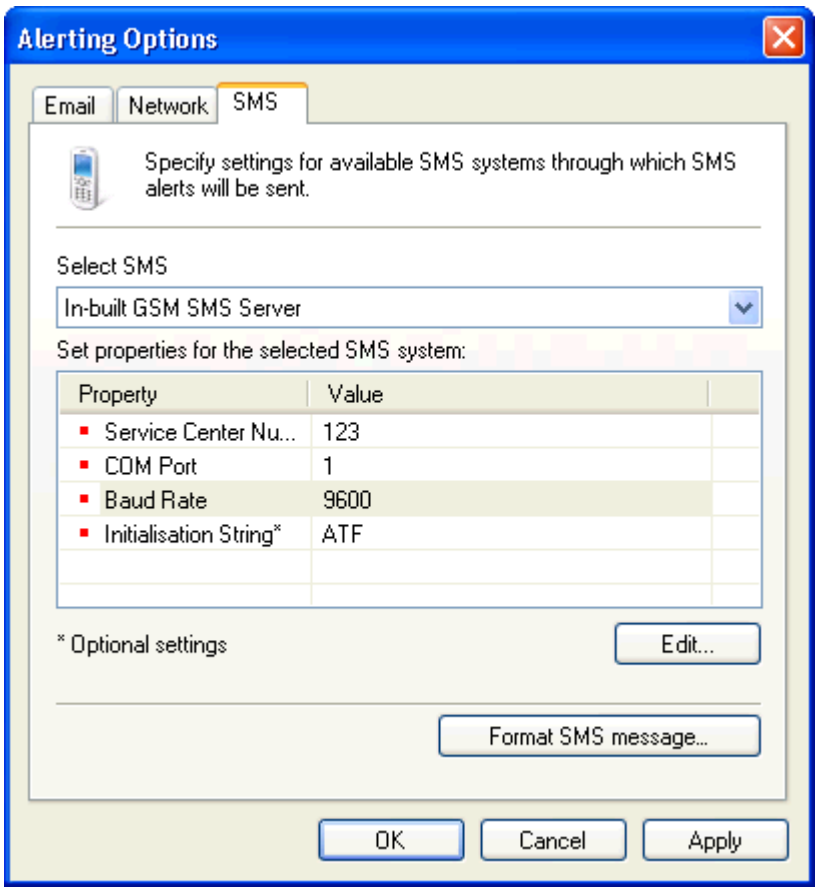
5. In the **Alerting Options** dialog select the **Email** tab.
6. Click **Add…** and key in the mail server settings and the authentication details if required and the details of the sender, and click **OK**.
7. To customize the email message text, click **Format Email Message…**, modify the **Subject** and **Message** fields as required, and click **Save**.


Alerting Options
Email
Network
SMS
Specify the network settings to use when sending network alerts.
Specify the network message settings to use when sending net send alerts to the computers used by the administrators of the machines which triggered any monitoring alerts.
Format network message...
Network messages can be sent to both computers and users. In the case of users, the user must be logged on so as to successfully receive the message. For both computers and users, the messenger service must be enabled and started.
OK
Cancel
Apply

Screenshot 108 - Alerting Options - Network tab

8. Select the **Network** tab.

9. To customize the network message text, click **Format network message…**, modify the **Subject** and **Message** fields as required, and click **Save**.



Screenshot 109 - Alerting Options - SMS tab

10. Select the **SMS** tab.

11. From the provided drop-down, select the SMS system through which SMS notifications will be sent. Supported SMS systems include:

- GFI FAXmaker SMS gateway
- Clickatell Email to SMS service gateway

12. Highlight the SMS system property to be configured from the list provided, click **Edit…**, modify the **Value** field as required, and click **OK**.

Repeat the preceding sub-step for each SMS system property you want to modify.

13. To customize the SMS message text, click **Format SMS message…**, modify the **Subject** and **Message** fields as required, and click **Save**.

14. Click **OK**.

10.5 Configuring alert recipients

GFI EndPointSecurity provides you with the facility to configure other profile accounts (apart from the default GFI EndPointSecurityAdministrator account) to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages.

Alert recipients are not Active Directory (AD) users and/or user groups, or local users and/or groups schema, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts.

10.5.1 Creating alert recipients

To create a new alert recipient:

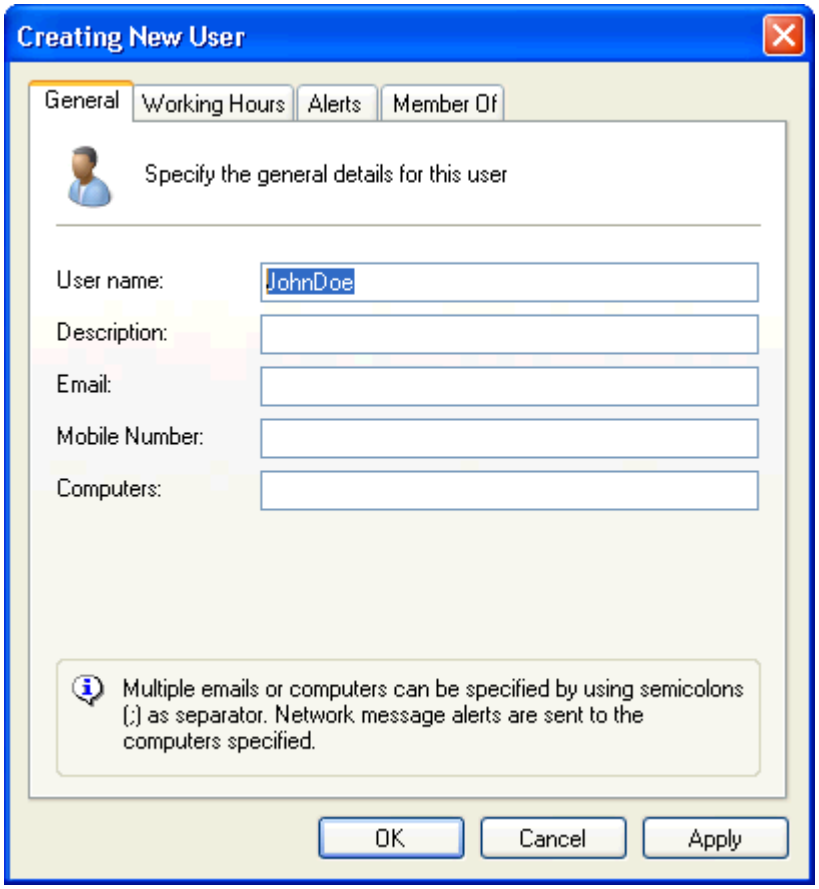
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Options** sub-tab.

3. Click on the **Alerting Options** node.

4. Click on the **Users** sub-node.

5. From the left pane, click the **Create user…** hyperlink in the **Common Tasks** section.



Screenshot 110 - Creating New User options - General tab

For more information on how to fill in the contents within the **Creating New User** dialog, refer to the Configuring the alerts administrator account section in this chapter.

6. Click **OK**.

10.5.2 Editing alert recipient properties

To edit an alert recipient's properties:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. Click on the **Users** sub-node.
5. From the right pane, highlight the required alert recipient's account.
6. From the left pane, click the **Edit selected user…** hyperlink in the **Actions** section.

For more information on how to edit the contents within the alert recipient's properties dialog, refer to the Configuring the alerts administrator account section in this chapter.

7. Click **OK**.

10.5.3 Deleting alert recipients

To delete an alert recipient:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. Click on the **Users** sub-node.
5. From the right pane, highlight the required alert recipient's account.

6. From the left pane, click the **Delete selected user** hyperlink in the **Actions** section, and click **Yes**.

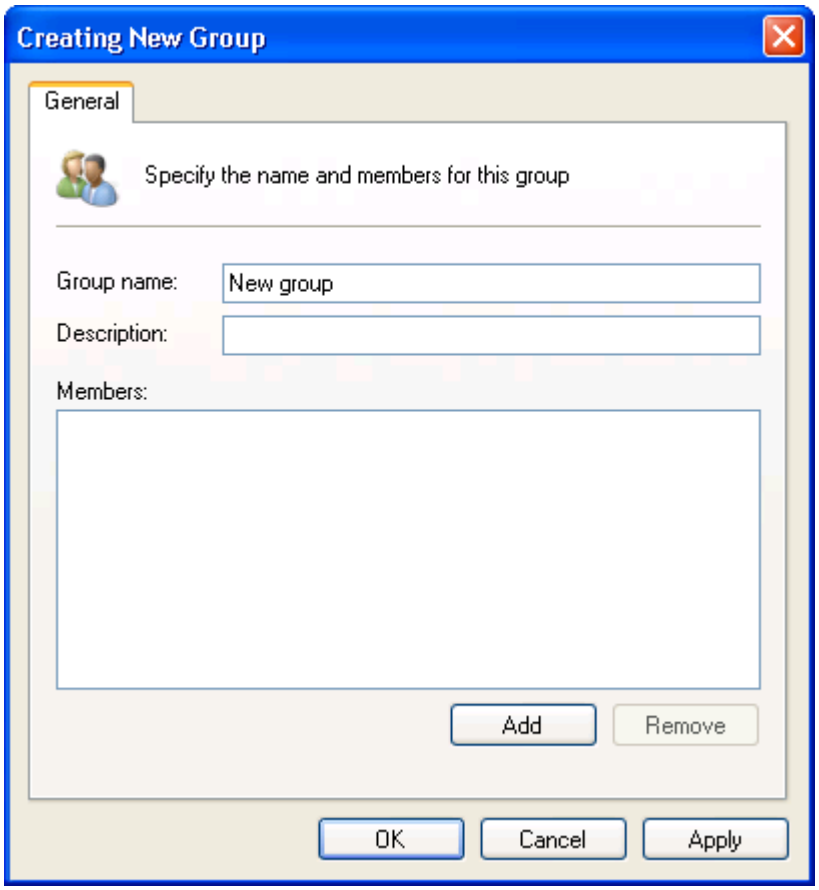
10.6 Configuring groups of alert recipients

GFI EndPointSecurity provides you with the facility to organize your alert recipients into groups in order to facilitate the management of alert recipients.

10.6.1 Creating groups of alert recipients

To create a new group of alert recipients:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. Click on the **Groups** sub-node.
5. From the left pane, click the **Create group…** hyperlink in the **Common Tasks** section.



Screenshot 111 - Creating New Group options

6. In the **Creating New Group** dialog key in the **Group name** and if required a **Description**.
7. Click **Add** to select the user(s) that belong to this notification group, and click **OK**.

10.6.2 Editing group of alert recipients properties

To edit group of alert recipients properties:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. Click on the **Groups** sub-node.
5. From the right pane, highlight the required group of alert recipients' account.
6. From the left pane, click the **Edit selected group…** hyperlink in the **Actions** section.

For more information on how to edit the contents within the group of alert recipients' properties dialog, refer to the **Creating groups of alert recipients** section in this chapter.

7. Click **OK**.

10.6.3 Deleting groups of alert recipients

To delete a group of alert recipients:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. Click on the **Groups** sub-node.
5. From the right pane, highlight the required group of alert recipients' account.
6. From the left pane, click the **Delete selected group** hyperlink in the **Actions** section, and click **Yes**.

10.7 Configuring digest report

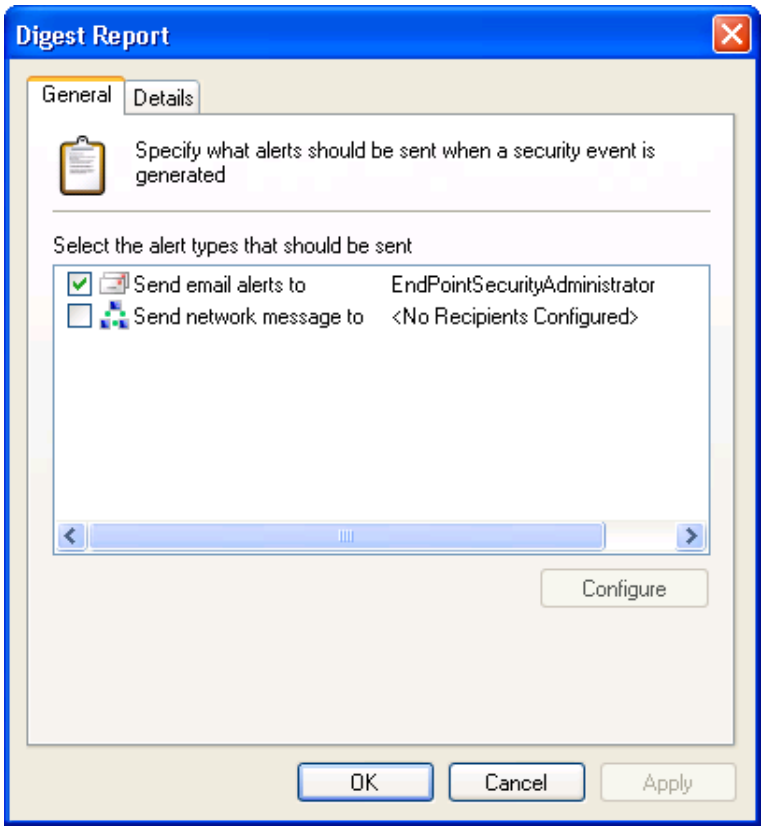
GFI EndPointSecurity provides you with the facility to configure the following options for a summary report, giving an account of the activity statistics as detected by GFI EndPointSecurity:

- alert types to be sent to the alert recipients
- contents of the report
- frequency of the report

Alert recipients are not Active Directory (AD) users and/or user groups, or local users and/or groups schema, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts. It is best to create alert recipients prior to configuring alerts. For more information on how to create the users and groups for notification purposes, refer to the **Configuring alert recipients** section in the **Customizing GFI EndPointSecurity** chapter.

To configure the digest report:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.
2. Click on the **Options** sub-tab.
3. Click on the **Alerting Options** node.
4. From the right pane, click the **Configure the digest report** hyperlink in the **Alerting Options** section.

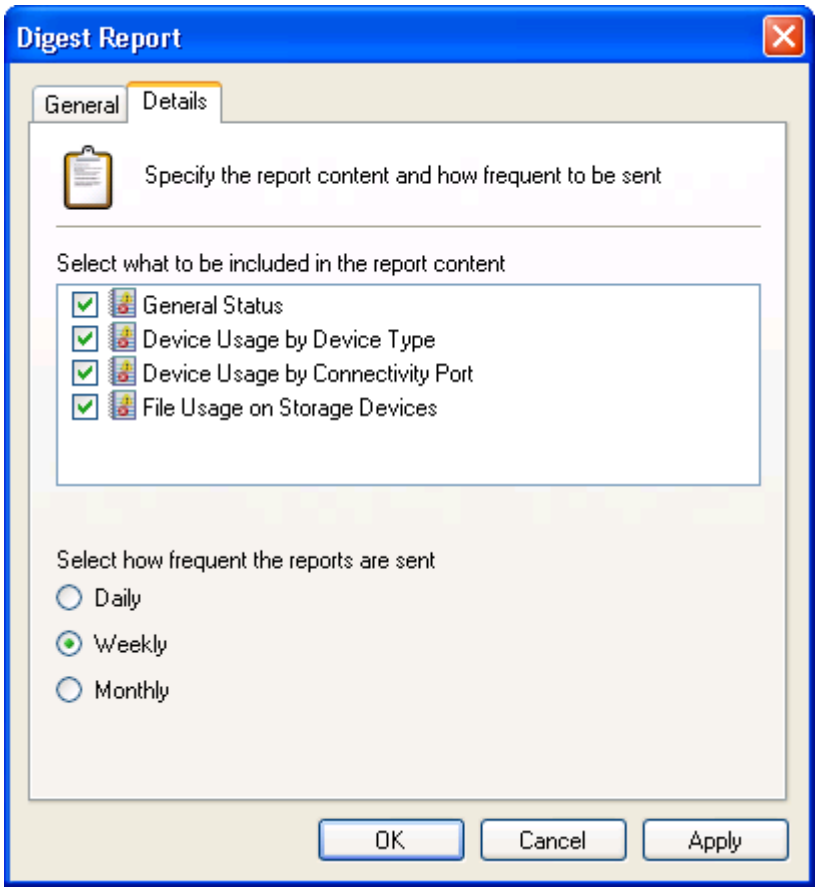


Screenshot 112 - Digest Report options - General tab

5. In the **Digest Report** dialog select the **General** tab.

6. Enable or disable the required alert types to be sent.

7. For each alert type enabled, highlight the alert type and click **Configure** to specify the user(s)/group(s) to whom the alert should be sent.



Screenshot 113 - Digest Report options - Details tab

8. Select the **Details** tab to specify the report content to be sent by GFI EndPointSecurity.

9. Enable or disable the report content items that are to be included within the alerts sent by GFI EndPointSecurity:

- General Status
- Device Usage by Device Type
- Device Usage by Connectivity Port
- File Usage on Storage Devices

10. Set frequency of the reports from **Daily**, **Weekly** or **Monthly**, and click **OK**.

10.8 Configuring database backend

GFI EndPointSecurity provides you with the facility to keep an audit trail of all events generated by GFI EndPointSecurity agents deployed on target computers.

After installing GFI EndPointSecurity you can choose to:

- Download and install an instance of Microsoft SQL Server Express Edition and to automatically create a database for GFI EndPointSecurity. This can be done through the Quick Start wizard.
- Connect to an available Microsoft SQL Server instance and then you can either connect to an existing database or else create a new one. This can be done through the Quick Start wizard, the General Status or the Options sub-tabs.

This section describes how to connect to an available Microsoft SQL Server instance through the General Status or the Options sub-tabs.

For more information on how to automatically download and install an instance of Microsoft SQL Server Express Edition or on how to connect to an available Microsoft SQL Server instance through the Quick Start wizard, refer to the GFI EndPointSecurity - Getting Started Guide.

10.8.1 Connecting to an available SQL Server instance

To access database backend settings:

Option 1: Access through the General sub-tab:

1. From the GFI EndPointSecurity management console, click on the **Status** tab.

2. Click on the **General** sub-tab.

3. Click on the **Configure database…** hyperlink in the **Database Backend Status** section.

Option 2: Access through the Options sub-tab:

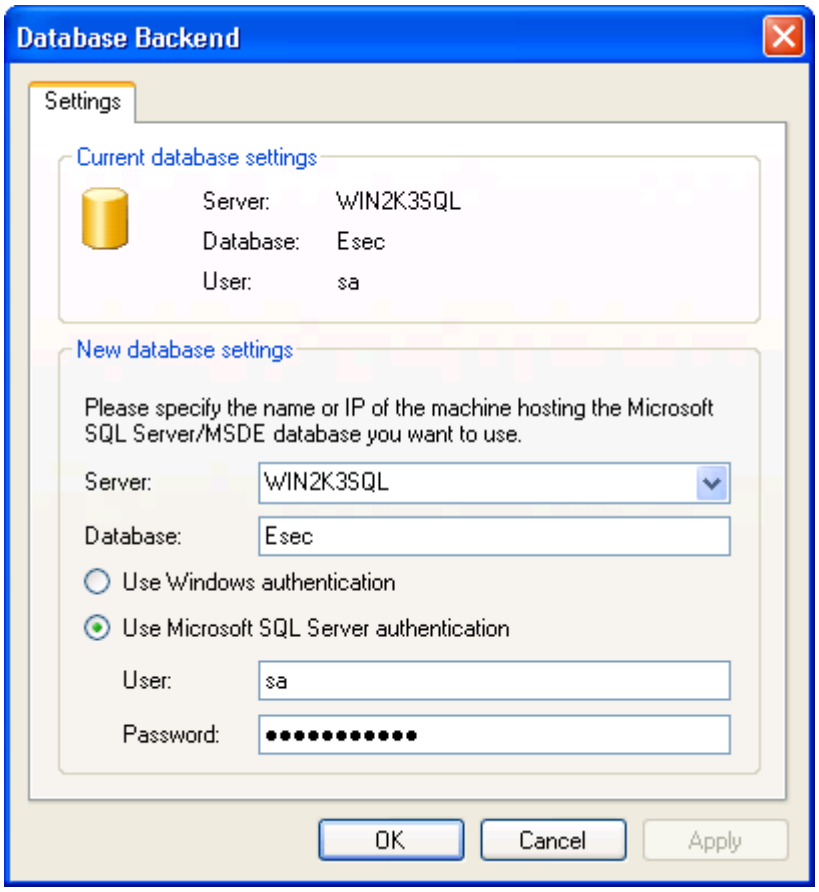
1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Options** sub-tab.

3. Click on the **Database Backend** node.

4. From the right pane, click the **Change database backend** hyperlink in the **Database backend** section.

To connect to an available SQL Server instance and either create a new database backend or change database backend settings:



Screenshot 114 - Database Backend options

1. In the **Database Backend** dialog select or key in the server name/IP address of an available database server or of a new SQL instance from the **Server** dropdown list.

2. Key in the database name in the **Database** field.

3. Select the authentication method to be used when connecting to the database backend server, and click **OK**.

If **Use Microsoft SQL Server authentication** is selected, key in the login username and password of the database backend server.

10.8.2 Maintaining the database backend

Periodical database maintenance is essential in order to prevent your database backend from growing too much. GFI EndPointSecurity provides you with the facility to configure parameters that automatically maintain your database backend.

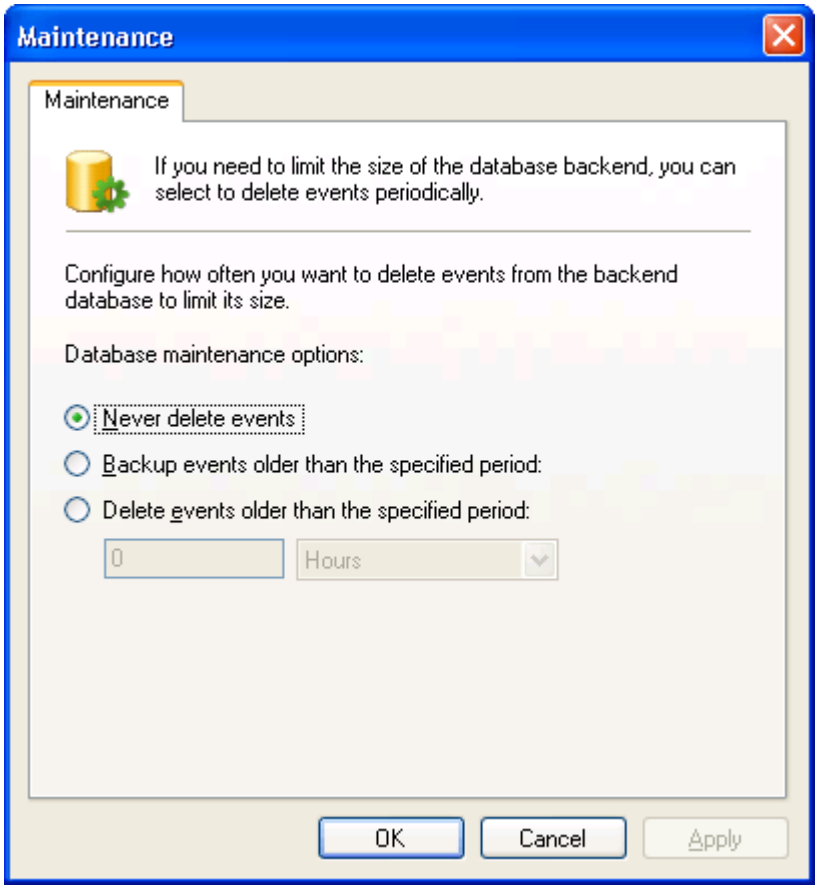
To configure database backend maintenance:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Options** sub-tab.

3. Click on the **Database Backend** node.

4. From the right pane, click the **Database maintenance** hyperlink in the **Database backend** section.


Maintenance
Maintenance
If you need to limit the size of the database backend, you can select to delete events periodically.
Configure how often you want to delete events from the backend database to limit its size.
Database maintenance options:
Never delete events
Backup events older than the specified period:
Delete events older than the specified period:
0
Hours
OK
Cancel
Apply

Screenshot 115 - Maintenance options

5. In the **Maintenance** dialog select the required database maintenance option from:

- **Never delete events**
- **Backup events older than the specified period** - specify the frequency in hours/days at which events will be backed up from the field and drop-down list provided. This option automatically moves events from the database backend to the backup database every time an events backup is performed.
- **Delete events older than the specified period** - specify the frequency in hours/days at which events will be deleted from the database backend from the field and drop-down list provided. Deleted records can NOT be recovered.

6. Click **OK**.

10.9 Configuring user messages

GFI EndPointSecurity provides you with the facility to customize the messages that will be displayed by the GFI EndPointSecurity agents on target computers, when devices are accessed.

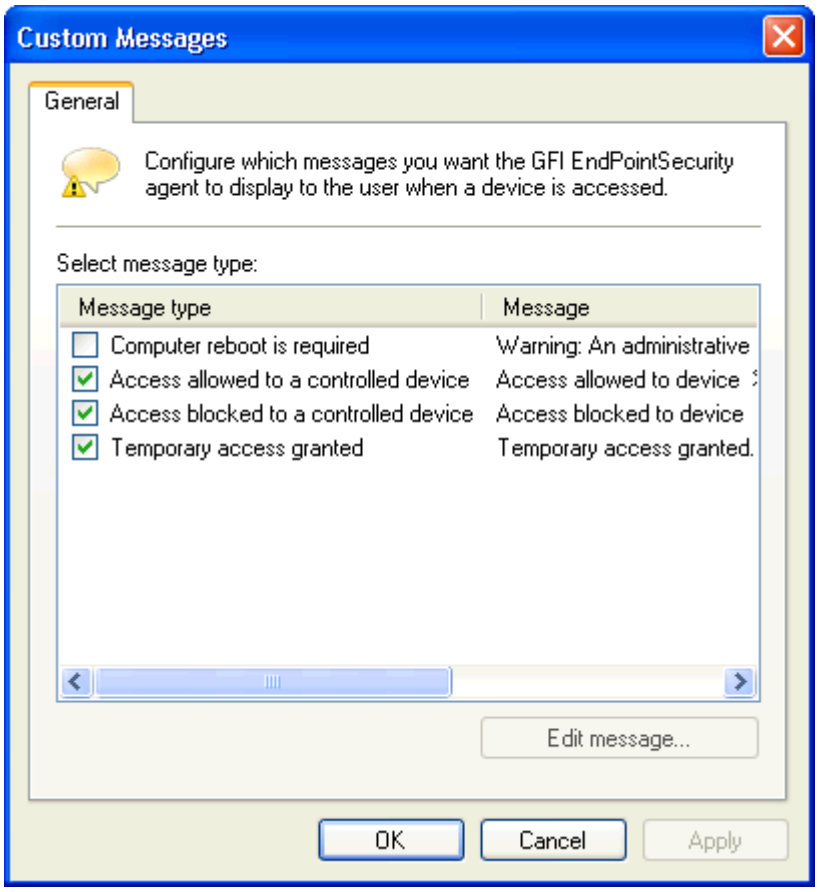
To customize these messages:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Options** sub-tab.

3. Click on the **Custom Messages** node.

4. From the right pane, click the **Customize user messages** hyperlink in the **Custom Messages** section.



Screenshot 116 - Custom Messages options

5. In the **Custom Messages** dialog enable or disable the required message types.

6. For each message type enabled, highlight the message type and click **Edit message…**, modify the text as required, and click **Save**.

Repeat the preceding sub-step for each message you want to modify.

7. Click **OK**.

10.10 Configuring advanced GFI EndPointSecurity options

GFI EndPointSecurity provides you with the facility to configure the following settings related to GFI EndPointSecurity agents:

- main communication TCP/IP port
- deployment options
- agents control password

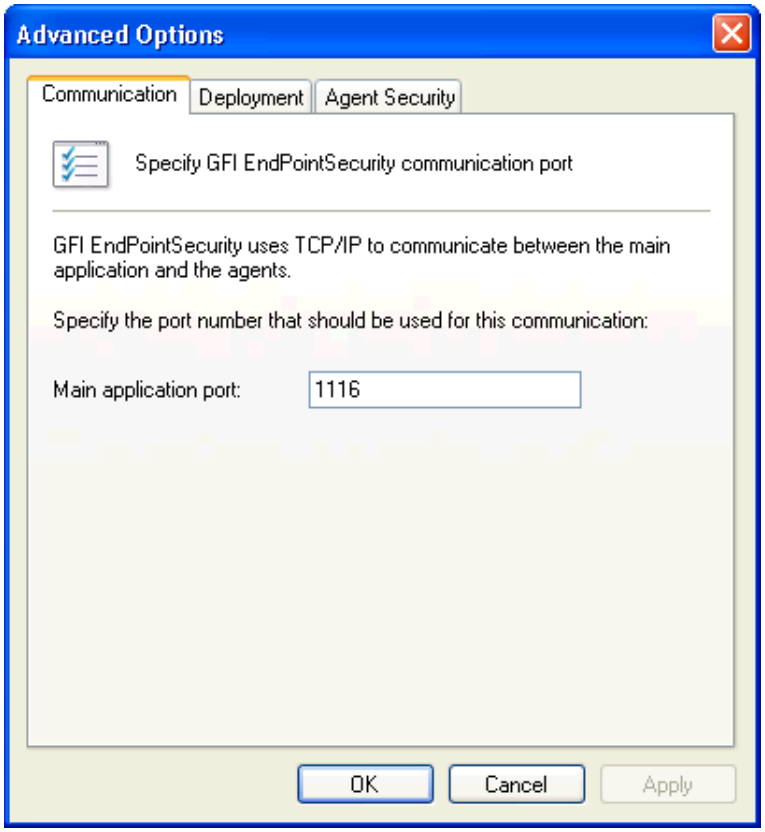
To configure the advance options:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Options** sub-tab.

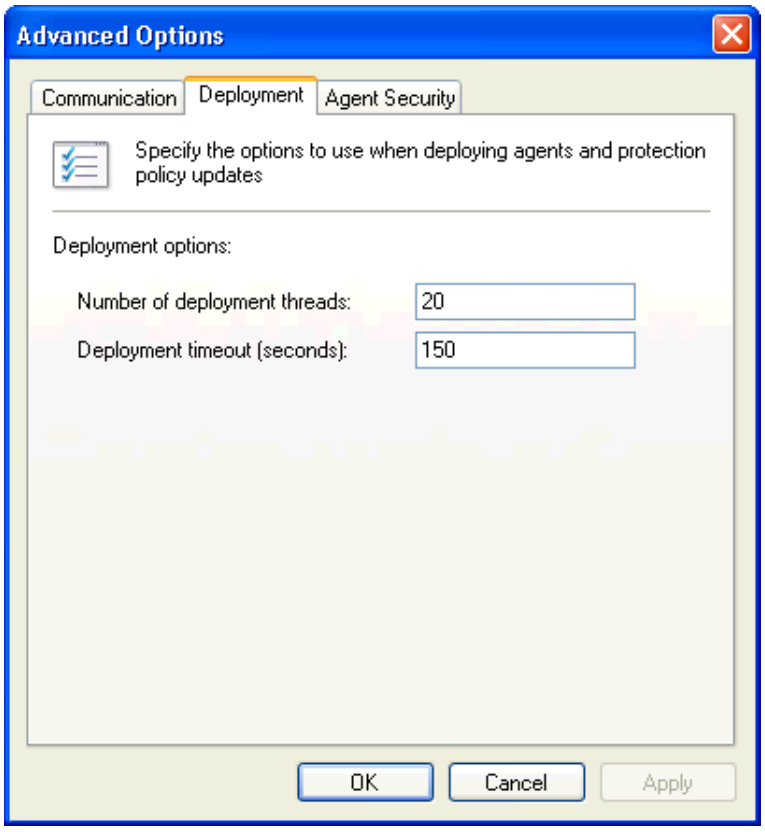
3. Click on the **Advanced Options** node.

4. From the right pane, click the **Modify advanced options** hyperlink in the **Advanced Options** section.



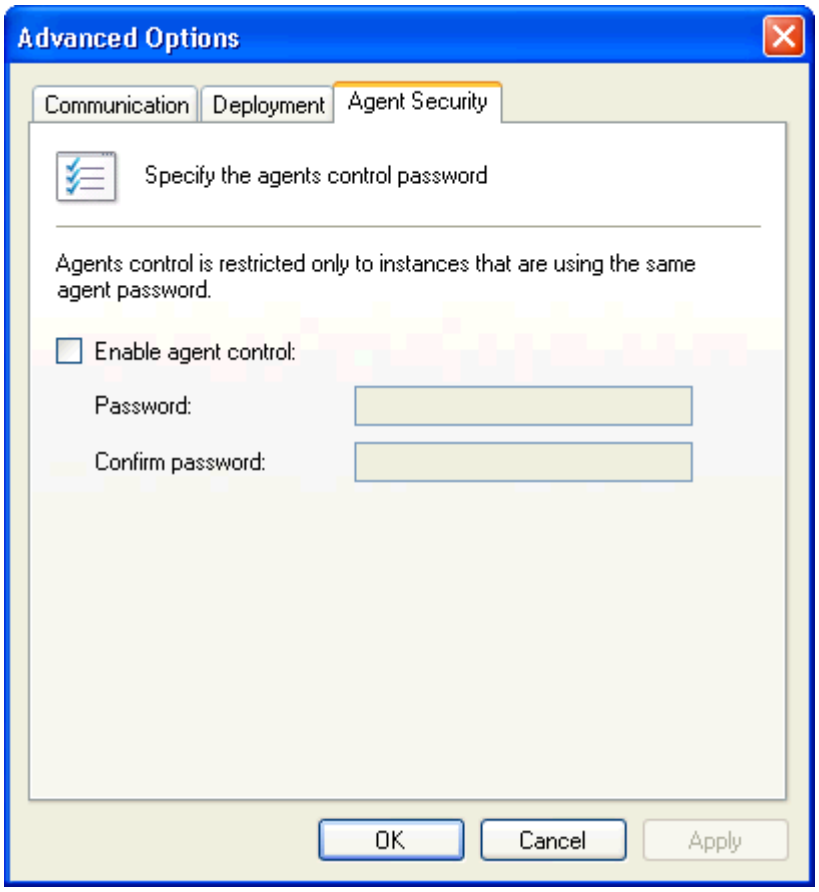
Screenshot 117 - Advanced Options - Communication tab

5. In the **Advanced Options** dialog select the **Communication** tab and key in the required TCP/IP port number to be used for communications between the GFI EndPointSecurity management console and the GFI EndPointSecurity agents (TCP/IP 1116 is the default port number).



Screenshot 118 - Advanced Options - Deployment tab

6. Select the **Deployment** tab and key in the required **Number of deployment threads** and **Deployment timeout (seconds)** values.



Screenshot 119 - Advanced Options - Agent Security tab

7. Select the **Agent Security** tab and enable or disable **Enable agent control**. If enabled, key in the agent password.

Only agents using the specified agents control password can be controlled.

8. Click **OK**.

11 Uninstalling GFI EndPointSecurity

11.1 Introduction

GFI EndPointSecurity enables you to easily uninstall both the GFI EndPointSecurity agents and the GFI EndPointSecurity application.

This chapter covers the following topics:

- Uninstalling GFI EndPointSecurity agents
- Uninstalling GFI EndPointSecurity application

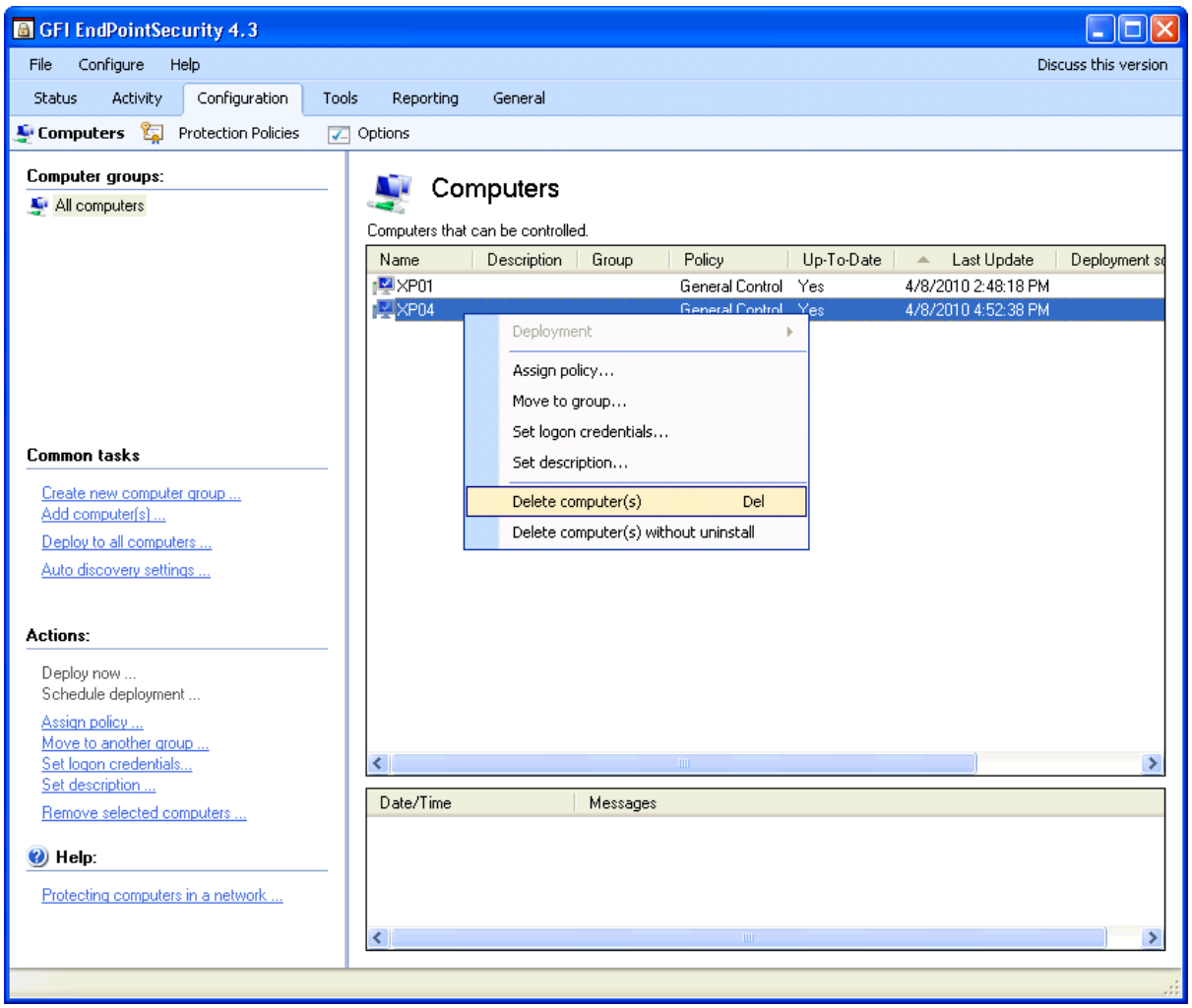
GFI EndPointSecurity agents are not uninstalled automatically during the un-installation of the GFI EndPointSecurity application. It is best that first you uninstall the GFI EndPointSecurity agents and next the GFI EndPointSecurity application.

11.2 Uninstalling GFI EndPointSecurity agents

To uninstall a GFI EndPointSecurity agent:

1. From the GFI EndPointSecurity management console, click on the **Configuration** tab.

2. Click on the **Computers** sub-tab.



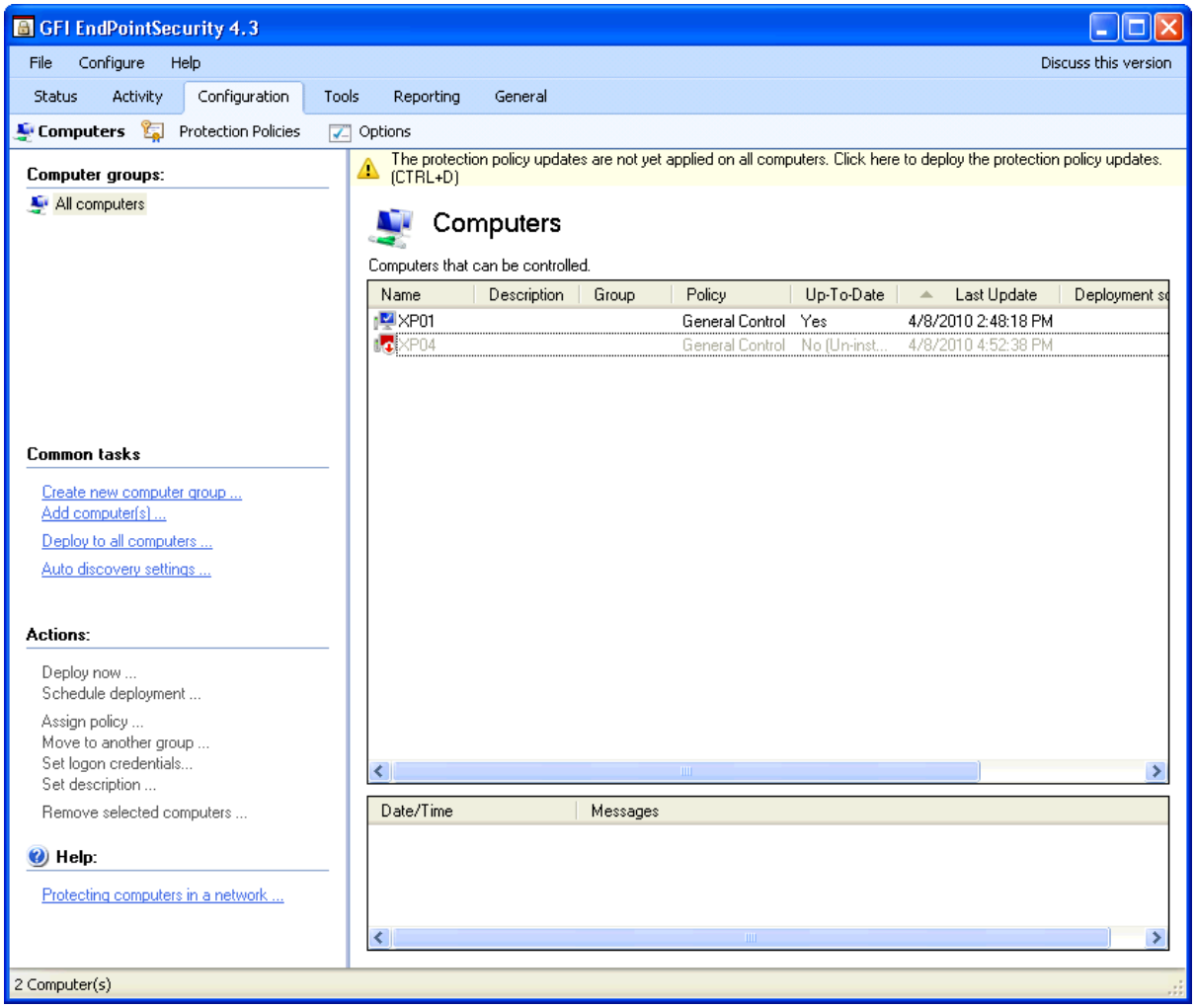
Screenshot 120 - Computers sub-tab - delete computer(s)

3. From the right pane, right-click on the target computer that you would like to uninstall and select:

- **Delete computer(s)** - will uninstall the GFI EndPointSecurity agent from the target computer, once the protection policy updates are deployed.

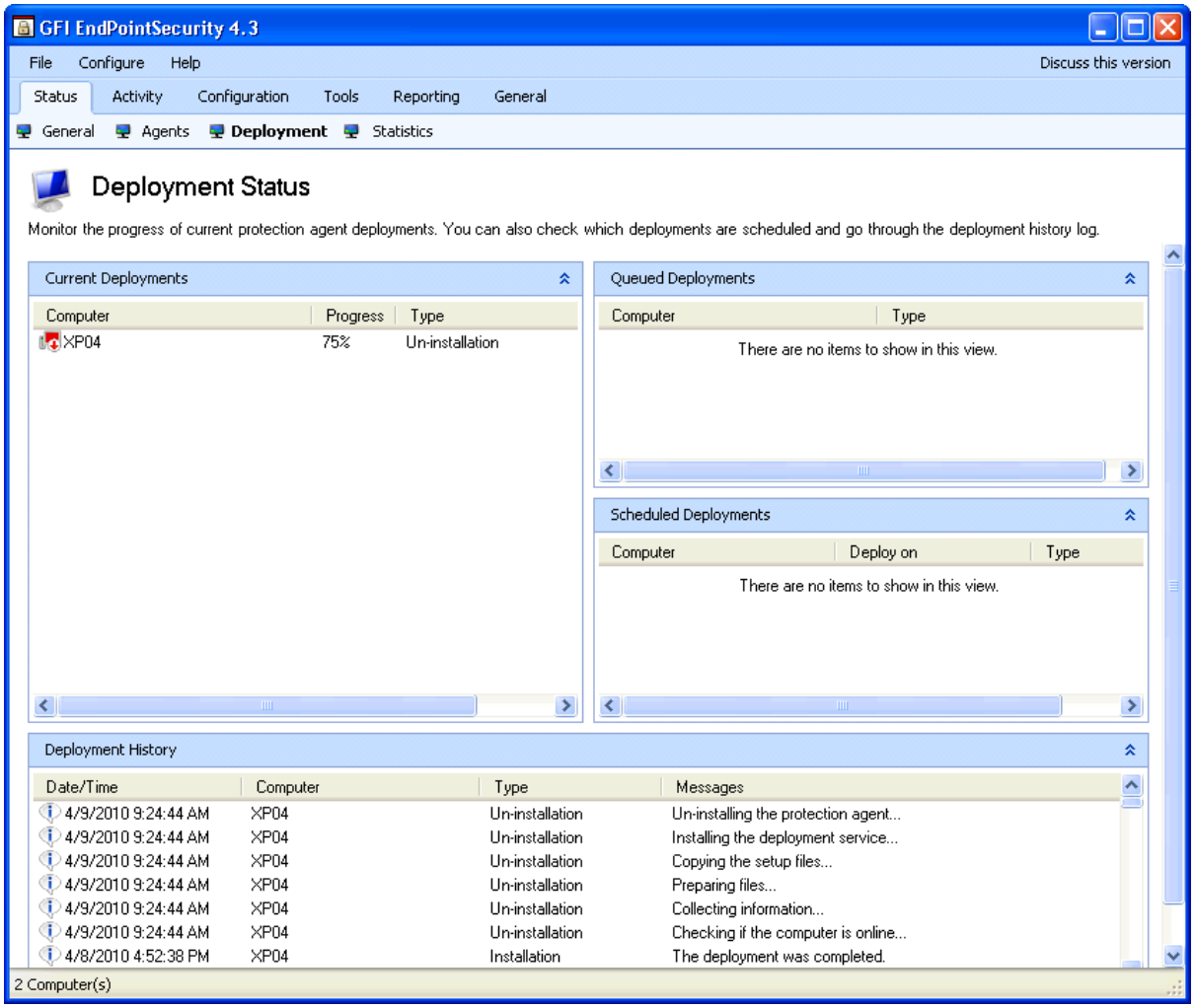
» **Delete computer(s) without uninstall** - will remove the relevant computer entry from the **Computers** list but will leave the agent installed on the target computer. This is useful in the event that the target computer was removed from the network and GFI EndPointSecurity application is unable to connect to it to uninstall the agent.

4. Click **Yes** to confirm the deletion of the selected computer from the list.



Screenshot 121 - Computers sub-tab - pending uninstall

5. From the right pane, click on the top warning message to deploy the protection policy updates. The view should automatically change to **Status ► Deployment**.


GFI EndPointSecurity 4.3
File Configure Help
Discuss this version
Status Activity Configuration Tools Reporting General
General Agents Deployment Statistics
Deployment Status
Monitor the progress of current protection agent deployments. You can also check which deployments are scheduled and go through the deployment history log.
Current Deployments
Computer Progress Type
XP04 75% Un-installation
Queued Deployments
Computer Type
There are no items to show in this view.
Scheduled Deployments
Computer Deploy on Type
There are no items to show in this view.
Deployment History
Date/Time Computer Type Messages
4/9/2010 9:24:44 AM XP04 Un-installation Un-installing the protection agent...
4/9/2010 9:24:44 AM XP04 Un-installation Installing the deployment service...
4/9/2010 9:24:44 AM XP04 Un-installation Copying the setup files...
4/9/2010 9:24:44 AM XP04 Un-installation Preparing files...
4/9/2010 9:24:44 AM XP04 Un-installation Collecting information...
4/9/2010 9:24:44 AM XP04 Un-installation Checking if the computer is online...
4/8/2010 4:52:38 PM XP04 Installation The deployment was completed.
2 Computer(s)

Screenshot 122 - Deployment sub-tab

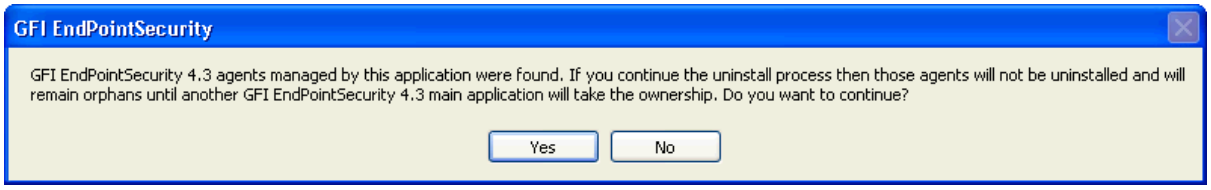
6. From the **Deployment History** area, confirm the successful completion of the un-installation from the target computer.

11.3 Uninstalling GFI EndPointSecurity application

To uninstall the GFI EndPointSecurity application:

Run the uninstaller as a user with administrative privileges on the computer.

1. From the **Microsoft Windows Control Panel** select **Add/Remove Programs** or **Programs and Features** option.
2. Select **GFI EndPointSecurity**.
3. Click **Change** to start the un-installation of GFI EndPointSecurity application.
4. Click **Next** at the Welcome screen to continue un-installation.


GFI EndPointSecurity
GFI EndPointSecurity 4.3 agents managed by this application were found. If you continue the uninstall process then those agents will not be uninstalled and will remain orphans until another GFI EndPointSecurity 4.3 main application will take the ownership. Do you want to continue?
Yes
No

Screenshot 123 - Un-installation information message

If any agents are still installed, an information dialog will be displayed asking you whether you would like to continue (the agents will remain installed and orphans) or stop the un-installation process. For more information about uninstalling agents, refer to the Uninstalling GFI EndPointSecurity agents section in this chapter.

5. Select **Uninstall without deleting configuration files** or **Complete uninstall** option and click **Next** to continue.

6. Upon un-installation completion click **Finish** to finalize un-installation.

12 Miscellaneous

12.1 Introduction

The miscellaneous chapter gathers all the other information that falls outside the initial configuration of GFI EndPointSecurity.

12.2 Entering your license key after installation

After installing GFI EndPointSecurity you can enter your license key without re-installing or re-configuring the application.

To enter your license key:

1. From the GFI EndPointSecurity management console, click on the **General** tab.
2. From the left pane select **Licensing**.
3. From the right pane, click the **(Edit …)** hyperlink in the **Licensing** section.

License Key
Enter the license key for GFI EndPointSecurity below. If you are evaluating the product do not enter a license key.
License key:
Evaluation
OK
Cancel

Screenshot 124 - License key editing message

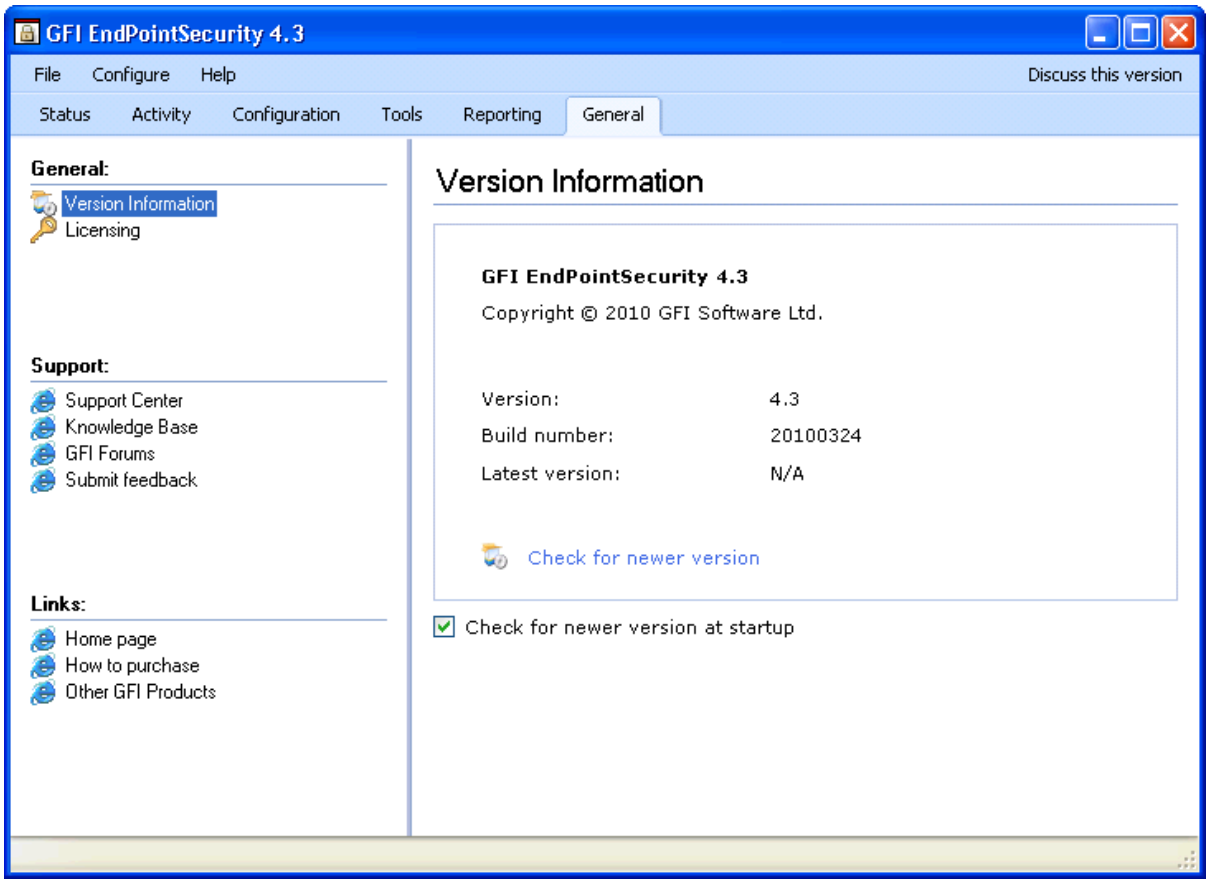
4. In the **License Key** text box, key in the license key provided by GFI Software Ltd.
5. Click **OK** to apply the license key.

12.3 Checking for newer GFI EndPointSecurity versions

GFI Software Ltd. releases product updates which can be manually or automatically downloaded from the GFI website.

To check if a newer version of GFI EndPointSecurity is available for download:

1. From the GFI EndPointSecurity management console, click on the **General** tab.
2. From the left pane, select **Version Information**.



Screenshot 125 - General tab - Version Information area

3. From the right pane click **Check for newer version** hyperlink to manually check if a newer version of GFI EndPointSecurity is available. Alternatively, enable the **Check for newer version at startup** checkbox to automatically check if a newer version of GFI EndPointSecurity is available for download every time GFI EndPointSecurity is launched.

13 Troubleshooting

13.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual - most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting the GFI Technical Support

13.2 Common Issues

Issue encountered	Solution
Errors are displayed within the **Status ► Deployment ► Deployment History** section upon deployment of GFI EndPointSecurity agents from the GFI EndPointSecurity management console.	For more information about error messages, possible causes and possible solutions, refer to the **Appendix 1 - Deployment error messages** chapter in this manual.

13.3 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit **http://kbase.gfi.com/**.

13.4 Web Forum

User to user technical support is available via the web forum. The forum can be found at: **http://forums.gfi.com/**.

13.5 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form from: **http://support.gfi.com/supportrequestform.asp**.
- **Phone:** To obtain the correct technical support phone number for your region please visit: **http://www.gfi.com/company/contact.htm.**

Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: **http://customers.gfi.com**.

We will answer your query within 24 hours or less, depending on your time zone.

13.6 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: **http://www.gfi.com/pages/productmailing.htm**.

13.7 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: **documentation@gfi.com**.

14 Glossary

Access permissions	A set of permissions (access, read and write) that are assigned to users and groups per device category, connectivity port or a specific device.
Active Directory	A technology that provides a variety of network services, including LDAP-like directory services.
Alert recipient	A GFI EndPointSecurity profile account to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages.
Alerts	A set of notifications (e-mail alerts, network messages or SMS messages) that are sent to alert recipients when particular events are generated.
Alerts administrator account	An alert recipient account that is automatically created by GFI EndPointSecurity upon installation.
Automatic discovery	A GFI EndPointSecurity feature to search and discover computers that were newly connected to the network at configured scheduled times.
BitLocker To Go	A Microsoft Windows 7 feature to protect and encrypt data on removable devices.
Connectivity port	An interface between computers and devices.
Create Protection Policy wizard	A wizard to guide you in the creation and configuration of new protection policies. Configuration settings include the selection of device categories and ports to be controlled and whether to block or allow all access to them. This wizard also allows the configuration of file-type based filters, encryption permissions as well as logging and alerting options.
Database backend	A database used by GFI EndPointSecurity to keep an audit trail of all events generated by GFI EndPointSecurity agents deployed on target computers.
Deployment error messages	Errors that can be encountered upon deployment of GFI EndPointSecurity agents from the GFI EndPointSecurity management console.
Device blacklist	A list of specific devices whose usage is blocked when accessed from all the target computers covered by the protection policy.
Device category	A group of peripherals organized in a category.
Device scan	A GFI EndPointSecurity feature to search for all devices that are or have been connected to the scanned target computers.
Device whitelist	A list of specific devices whose usage is allowed when accessed from all the target computers covered by the protection policy.
Digest report	A summary report giving an account of the activity statistics as detected by GFI EndPointSecurity.
Event logging	A feature to record events related to attempts made to access devices and connection ports on target computers and service operations.
File-type filters	A set of restrictions that are assigned to users and groups per file-type. Filtering is based on file extension checks and real file type signature checks.
GFI EndPointSecurity agent	A client-side service responsible for the implementation/enforcement of the protection policies on the target computer(s).
GFI EndPointSecurity application	A server-side security application that aids in maintaining data integrity by preventing unauthorized access and transfer of content to and from devices and connection ports.
GFI EndPointSecurity management console	The user interface of the GFI EndPointSecurity server-side application.
GFI EndPointSecurity Temporary Access tool	A tool which is available on the target computers. It is used by the user to generate a request code and later to enter the unlock code in order to activate the temporary access once it is granted by the administrator. Upon activation, the user will have access to devices and connection ports (when such access is normally blocked) on his protected target computer for the specified duration and time window.

Global permissions	A Create Protection Policy wizard step that prompts the user to either block or else to allow access to all devices falling in a category or which are connected to a port of the target computers covered by the protection policy.
GPO	See Group Policy Objects.
Group Policy Objects	An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.
Human Interface Devices	A specification that is part of the universal serial bus (USB) standard for a class of peripheral devices. These devices, such as a mice, keyboards, and joysticks, enable users to input data or to interact directly with the computer.
MSI file	A file generated by GFI EndPointSecurity for later deployment using GPO or other deployment options. It can be generated for any protection policy and contains all the relevant configured security settings, including installation settings for unprotected target computers.
Power user	A power users is automatically given full access to devices connected to any target computer covered by the protection policy.
Protection policy	A set of device access and connectivity port permissions that can be configured to suit your company's device access security policies.
Quick Start wizard	A wizard to guide you in the configuration of GFI EndPointSecurity with custom settings. It is launched upon the initial launch of GFI EndPointSecurity management console and is intended for first time use.
Security encryption	A set of restrictions configured to either block or else to allow users/groups to access specific file-types stored on devices that are encrypted with BitLocker To Go. These restrictions are applied when the encrypted devices are connected to the target computers covered by the protection policy.
Target computer	A computer that is protected by a GFI EndPointSecurity protection policy.
Temporary access	A period of time during which users are allowed to access devices and connection ports (when such access is normally blocked) on protected target computers, for a specified duration and time window.
User message	A message that is displayed by GFI EndPointSecurity agents on target computers, when devices are accessed.

15 Appendix 1 - Deployment error messages

15.1 Introduction

This section provides a list of errors that can be encountered when deploying agents or protection policies, possible causes for these errors and possible solutions. The deployment status can be accessed from the GFI EndPointSecurity management console by navigating to **Status ► Deployment ► Deployment History**.

15.2 Deployment error messages

In the following table, some error messages are in the format “GFI EndPointSecurity error (system error)”. The errors within the parenthesis are reported by the system and may vary according to the cause of the error.

Message	Possible causes	Possible solutions
The computer is offline.	GFI EndPointSecurity management console pings the target computer at deployment to determine whether it is online, and if not this message is displayed.	If a target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecurity keeps trying to deploy that policy every hour, until the target computer is back online. Ensure that the target computer is switched on and connected to the network.
Failed to connect to the remote registry. (error)	GFI EndPointSecurity was not able to extract data from the registry of the target computer.	Ensure that your firewall settings enable communication between the target computers and the GFI EndPointSecurity server.
Failed to gather required information. (error)	GFI EndPointSecurity was not able to extract version related data from the target computer (Operating System version and GFI EndPointSecurity agent version).	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.
Failed to build the required installation files. (error)	GFI EndPointSecurity was not able to add the necessary configuration files within the deployment file (.msi installation file) of the GFI EndPointSecurity agent. This error occurs before the deployment file is copied onto the target computer.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.

Message	Possible causes	Possible solutions
Failed to copy the files to the remote computer. (error)	GFI EndPointSecurity was not able to copy the deployment file (.msi installation file) onto the target computer. A possible cause can be that, the administrative share (C$) that GFI EndPointSecurity is using to connect to the target computer, is disabled.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis. For further information about network connectivity and security permissions, refer to: http://kbase.gfi.com/showarticle.asp?id=KBID003754
Timeout	Agent deployment onto the target computer is either taking too long to complete or else is blocked..	Please try to deploy the GFI EndPointSecurity agent again.
Failed to install the deployment service. (error)	The GFI EndPointSecurity agent was not able to be installed or uninstalled by the service running on the target computer.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.
Installation failed.	Installation of the GFI EndPointSecurity agent is complete, but is not marked as installed within the registry. The version and build numbers of the GFI EndPointSecurity agent are not the same as those of the GFI EndPointSecurity management console.	For more details about the cause of the error and a possible solution, refer to the agent installation log files on the target computer at: %windir%\EndPointSecurity.
Un-installation failed.	Un-installation of the GFI EndPointSecurity agent is complete, but is not marked as uninstalled within the registry.	For more details about the cause of the error and a possible solution, refer to the agent installation log files on the target computer at: %windir%\EndPointSecurity.
The operation failed due to an unknown exception.	GFI EndPointSecurity has encountered an unexpected error.	Please use the Troubleshooter Wizard to contact the GFI Technical Support team. To open the Troubleshooter Wizard navigate to **Start ► Programs ► GFI EndPointSecurity 4.3 ► GFI EndPointSecurity 4.3 Troubleshooter**.

Index

A

access permissions, 121

- connectivity ports, 65
- device categories, 62
- specific devices, 67
- viewing, 70

Active Directory, 6, 121

Activity Log sub-tab, 39

- advanced filtering, 39

Activity tab, 38

adding discovered devices in devices database, 57

advanced GFI EndPointSecurity options, 110

Agents sub-tab, 47

- Agents' Status area, 36

alert recipients, 102, 121

alerting options, 100

alerts, 87, 121

alerts administrator account, 97, 121

auto discovery settings, 93

automatic discovery, 121

B

BitLocker To Go, 5, 20, 84, 121

Build notifications, 119

C

Common Issues, 119

connecting to an available SQL Server instance, 107

connectivity port, 121

connectivity ports access permissions, 65

controlled categories and ports, 14

controlled connectivity ports, 60

controlled device categories, 59

Create Protection Policy wizard, 13, 121

- Alerting options, 24
- Controlled Connectivity Ports, 16
- Controlled Device Categories, 15
- Encryption, 19
- File-Type Filter, 18
- Logging options, 22

creating new protection policies, 13

customizing GFI EndPointSecurity, 93

customizing protection policies, 59

D

database backend, 107, 121

- connecting to an available SQL Server instance, 107
- maintaining the database backend, 108

deploying protection policies, 29

- Active Directory deployment, 35
- adding target computer, 29
- assigning a protection policy, 32
- configuring log on credentials, 31
- deploying a protection policy, 33
- immediate deployment, 33
- scheduled deployment, 34
- verifying deployment, 35

deployment error messages, 121, 123

Deployment sub-tab, 48

- Current Deployments area, 49
- Deployment History area, 35, 50
- Queued Deployments area, 50
- Scheduled Deployments area, 50

device blacklist, 5, 72, 121

device category, 121

device category access permissions, 62

Device Scan, 121

Device Scan results, 56

Device Scan sub-tab, 53

- Computers area, 56

Devices list area, 56

device whitelist, 5, 75, 121

digest report, 105, 121

discovering devices, 53

E

EndPointSecurityAdministrator account, 97

EndPointSecurityAdministrators notification group, 97

event logging, 85, 121

F

file-type filters, 81, 121

G

General sub-tab, 43

Agents' Status area, 46

Alerting Status area, 44

Database Backend Status area, 44

Device Usage area, 47

General Status area, 45

Online Status area, 46

Protection Status area, 45

Service Status area, 44

GFI EndPointSecurity

agent, 7, 121

application, 121

management console, 6, 121

Temporary Access tool, 10, 121

GFI EndPointSecurity - Getting Started Guide, 2

GFI EndPointSecurity ReportPack, 51

GFI ReportCenter, 51

global permissions, 16, 122

Glossary, 121

GPO *(Group Policy Objects)*, 122

granting temporary access, 79

groups of alert recipients, 104

H

How GFI EndPointSecurity works

deployment and monitoring, 7

device access, 9

temporary access, 9

Human Interface Devices, 16, 60, 122

K

Knowledge Base, 119

L

licensing, 3, 117

logging and alerting options, 21

Logs Browser sub-tab, 40

creating event queries, 41

M

maintaining the database backend, 108

monitoring device usage activity, 37

monitoring statuses, 43

msi file, 6, 35, 122, 123, 124

N

navigating the Management console, 11

P

policy name, 13

power users, 61, 122

priorities for permissions, 71

protection policy, 122

Q

Quick Start wizard, 122

R

ReportCenter, 51

reporting, 51

ReportPack, 51

requesting temporary access, 78

running a Device Scan, 53

S

security encryption, 83, 122

setting a policy as the default policy, 90

specific device access permissions, 67

Statistics sub-tab, 37, 50

Device Usage by Connectivity Port area, 38

Device Usage by Device Type area, 38

Protection Status area, 38

storage devices, 17

supported connectivity ports, 11

supported device categories, 10

T

target computer, 122

Technical Support, 119

temporary access, 122

granting, 79

requesting, 78

temporary access privileges, 78

Troubleshooter wizard, 124

Troubleshooting, 119

U

uninstalling GFI EndPointSecurity, 113

agents, 113

application, 115

user messages, 109, 122

V

versions

checking for newer versions, 117

viewing access permissions, 70

W

Web Forum, 119

wizard

Create Protection Policy wizard, 13, 121

Quick Start wizard, 122

Troubleshooter wizard, 124

USA, CANADA, CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

Email: ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

Email: sales@gfiap.com

GFI®